NUCLEAR SECURITY: HAS THE NRC STRENGTHENED FACILITY STANDARDS SINCE SEPTEMBER 11TH?

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

APRIL 4, 2006

Serial No. 109–196

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

30–694 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

CHRISTOPHER SHAYS, Connecticut
DAN BURTON, Indiana
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
GIL GUTKNECHT, Minnesota
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, JR., Tennessee
CANDICE S. MILLER, Michigan
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
JON C. PORTER, Nevada
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
CHARLES W. DENT, Pennsylvania
VIRGINIA FOXX, North Carolina
JEAN SCHMIDT, Ohio

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. DUTCH RUPPERSBERGER, Maryland
BRIAN HIGGINS, New York
ELEANOR HOLMES NORTON, District of Columbia

BERNARD SANDERS, Vermont
(Independent)

DAVID MARIN, *Staff Director*
LAWRENCE HALLORAN, *Deputy Staff Director*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND INTERNATIONAL RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

KENNY MARCHANT, Texas
DAN BURTON, Indiana
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEVEN C. LATOURETTE, Ohio
TODD RUSSELL PLATTS, Pennsylvania
JOHN J. DUNCAN, JR., Tennessee
MICHAEL R. TURNER, Ohio
JON C. PORTER, Nevada
CHARLES W. DENT, Pennsylvania

DENNIS J. KUCINICH, Ohio
TOM LANTOS, California
BERNARD SANDERS, Vermont
CAROLYN B. MALONEY, New York
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. DUTCH RUPPERSBERGER, Maryland
STEPHEN F. LYNCH, Massachusetts
BRIAN HIGGINS, New York

EX OFFICIO

TOM DAVIS, Virginia
HENRY A. WAXMAN, California

LAWRENCE J. HALLORAN, *Staff Director and Counsel*
J. VINCENT CHASE, *Chief Investigator*
ROBERT A. BRIGGS, *Clerk*
ANDREW SU, *Minority Professional Staff Member*

CONTENTS

NUCLEAR SECURITY: HAS THE NRC STRENGTHENED FACILITY STANDARDS SINCE SEPTEMBER 11TH?

TUESDAY, APRIL 4, 2006

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:05 p.m., in room 2247, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representative Shays, Platts, Duncan, Kucinich, and Van Hollen.

Staff present: Lawrence Halloran, staff director and counsel; R. Nicholas Palarino, Ph.D., senior policy advisor; Robert A. Briggs, analyst; Marc LaRoche, intern; Andrew Su, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. SHAYS. A quorum being present, the Subcommittee on National Security, Emerging Threats, and International Relations hearing entitled, "Nuclear Security: Has The NRC Strengthened Facility Standards Since September 11th?" is called to order.

This afternoon, the subcommittee continues our oversight of security standards at civilian nuclear power facilities. Twice before, we convened to measure the scope and pace of post September 11th safeguard improvements in and around reactor sites. Both hearings found some progress, revisited enduring challenges, and elicited promises of tangible progress.

Today, we take account of those commitments and ask specifically how the Nuclear Regulatory Commission [NRC], and the nuclear power industry are maintaining readiness against a changing threat. One necessary security tool, secrecy, prevents an open discussion of some particular elements of the design basis threat [DBT], which sets the threshold of enemies and capabilities against which reactor sites should be able to defend.

We will convene a closed session next month to give Members access to classified material and nuclear safeguard information supporting the DBT. But the most important part of this conversation is about public safety, public health, and the protection of critical infrastructure. It can and should take place in the open.

At our request, the Government Accountability Office [GAO] conducted an in-depth examination of the process used by the NRC to update the design basis threat standard, the industry response to

new security mandates, and the rigor of inspections and drills used to test security force readiness.

The GAO findings, released today, painted a decidedly mixed picture of nuclear power security. Substantial improvements have been made since September 11, 2001, and since adoption of the new design basis threat in 2003. Buffer zones have been augmented where possible, barriers have been thickened, detection equipment installed or upgraded. Protective forces have been enlarged and armed with new weapons and smarter strategies.

But according to GAO, it may be too early to claim success since fewer than half of the 65 NRC-regulated sites have been tested against a live adversary in what are called force-on-force exercises. Additionally those tested did not always perform as well as expected, even in necessarily artificial, fully noticed drills conducted in broad daylight.

GAO also found that stronger security standards did not necessarily mean the NRC had sufficiently fortified itself against the dangers of an overly cozy relationship with the industry. While still drafting the new design basis threat, the Commission solicited outside comments, creating the appearance industry was influencing the threat assessment process with extraneous cost concerns.

The regulated should never even appear to be able to dictate security standards to the regulator. But this is more than a question of appearance. Only the rigor and independence of the NRC process guarantee the integrity of the product.

Nevertheless, the Commission continues to resist the GAO recommendation to develop explicit criteria for decisions altering design basis threat standards. When the reasons for the NRC decision can only be guessed at, the commission should not be surprised when their critics see those actions as arbitrary or the product of undue outside influence.

We know the September 11th terrorists had their sights on a nuclear reactor. If they had succeeded in causing a radioactive release by breaching a containment facility with a truck bomb or draining the water from a fuel storage pool, how would this discussion be different? That is the conversation we need to have today.

So we welcome all our witnesses. They are experts, and they are dedicated to their work. We appreciate that a great deal, and we look forward to their testimony.

[The prepared statement of Hon. Christopher Shays follows:]

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382

Statement of Rep. Christopher Shays
April 4, 2006

This afternoon the Subcommittee continues our oversight of security standards at civilian nuclear power facilities. Twice before, we convened to measure the scope and pace of post-9/11 safeguard improvements in and around reactor sites. Both hearings found some progress, revisited enduring challenges and elicited promises of tangible progress. Today, we take account of those commitments and ask specifically how the Nuclear Regulatory Commission (NRC) and the nuclear power industry are maintaining readiness against a changing threat.

One necessary security tool, secrecy, prevents an open discussion of some particular elements of the Design Basis Threat, or DBT, which sets the threshold of enemies and capabilities against which reactor sites should be able to defend. We will convene a closed session next month to give Members access to classified material and nuclear safeguards information supporting the DBT. But the most important part of this conversation is about public safety, public health and the protection of critical infrastructure. It can, and should, take place in the open.

At our request, the Government Accountability Office (GAO) conducted an in-depth examination of: the process used by the NRC to update the Design Basis Threat standard, the industry response to new security mandates and the rigor of inspections and drills used to test security force readiness.

The GAO findings released today paint a decidedly mixed picture of nuclear power security. Substantial improvements have been made since September 11, 2001, and since adoption of the new DBT in 2003. Buffer zones have been augmented where possible, barriers have been thickened, detection equipment installed or upgraded. Protective forces have been enlarged and armed with new weapons and smarter strategies. But, according to GAO, it may too early to claim success since fewer than half the 65 NRC-regulated sites have been tested against a live adversary in what are called force-on-force exercises. And those tested did not always perform as well as expected, even in necessarily artificial, fully noticed drills conducted in broad daylight.

GAO also found that stronger security standards did not necessarily mean the NRC had sufficiently fortified itself against the dangers of an overly cozy relationship with the industry. While still drafting the new Design Basis Threat, the Commission solicited outside comments, creating the appearance industry was influencing the threat assessment process with extraneous cost concerns. The regulated should never even appear to be able to dictate security standards to the regulator. But this is more than a question of appearance. Only the rigor and independence of the NRC process guarantee the integrity of the product. Nevertheless, the Commission continues to resist the GAO recommendation to develop explicit criteria for decisions altering DBT standards. When the reasons for NRC decisions can only be guessed at, the Commission should not be surprised when their critics see those actions as arbitrary or the product of undue outside influence.

We know the 9/11 terrorists had their sights on a nuclear reactor. If they had succeeded in causing a radioactive release by breaching a containment facility with a truck bomb or draining the water from a fuel storage pool, how would this discussion be different? That is the conversation we need to have today.

Welcome to all our witnesses. We look forward to their testimony.

Mr. SHAYS. So at this time, let me welcome Mr. Jim Wells, Director, Natural Resources and Environment, Government Accountability Office; the Honorable Nils Diaz, chairman, U.S. Nuclear Regulatory Commission, accompanied by the Honorable Edward McGaffigan, Jr., Commissioner; and the Honorable Jeffrey S. Merrifield, Commissioner.

we look forward to the testimony and the response by all the folks there in terms of the questions that will be asked.

If I could, I know it is a tight seat, and I don't want to knock over the water again. But I would like you to stand up, and I will swear you in.

[Witnesses sworn.]

Mr. SHAYS. We will note for the record that all our witnesses have responded in the affirmative. Again, we welcome each of you.

And Mr. Wells, we will start with you.

STATEMENTS OF JIM WELLS, DIRECTOR, NATURAL RESOURCES AND ENVIRONMENT, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; NILS DIAZ, CHAIRMAN, U.S. NUCLEAR REGULATORY COMMISSION, ACCOMPANIED BY EDWARD McGAFFIGAN, JR., COMMISSIONER; AND JEFFREY S. MERRIFIELD, COMMISSIONER

STATEMENT OF JIM WELLS

Mr. WELLS. Thank you, Mr. Chairman.

We are pleased to be here today to discuss the GAO report on NRC's ability to assure the public and the Congress that nuclear power plants are capable of defending against a terrorist attack.

As you know, nuclear power plants were thought to be a target around the September 11th timeframe, and our sources believe power plants continue to be a general creditable threat target today.

Mr. Chairman, the process NRC used to decide on what level of security they thought was needed was, in our opinion, a well-defined and generally logical process. However, we did take issue with how they used some of their staff resources to gather information from the industry and the public as it related to the timing of making the decisions about what was to be in or what was to be out of the final DBT.

For example, some NRC staff, the same NRC staff that was responsible for assessing the available intelligence and making recommendations to NRC management was also used to obtain industry objections and the public. These objections ranged from such requirements being prohibitively expensive or excessive in the view that such a threat was coming from an enemy of the United States, therefore, a responsibility of the Government and not one for a private company.

The timing of how/when these decisions by the threat assessment staff on what DBT levels to recommend could create the appearance of a change being based on industry objectives, objections rather than an assessment of the terrorist threat. We believe that the best approach would be to insulate the same threat assessment staff from such interactions, allowing their recommendations to be

fact-based analysis of the threat instead of their involvement with policy-level considerations.

We also raised some concerns about the clarity and the transparency and the discretionary latitude given the Commissioners and how they cast their votes as to what weapon or what level of force was to be required in the DBT. The process that we evaluated in terms of what we saw in developing the DBT reveals that the Commissioners largely supported the staff's recommendations, but also they made significant changes.

Some things were not added, like defense against two types of weapons, bomb sizes, or quantities of equipment and explosives that could plausibly be used against a plant. We spoke with the Commissioners. We examined the voting records. We accepted the Commissioners' statements that their votes reflected their policy judgments and their legal authority as Commissioners.

In voting, the individual Commissioners used differing criteria, emphasized differing factors, such as the cost or the practicality of defensive measures. Our concern and our recommendation was not that the decisions may have been wrong, but that the criteria that would perhaps help or guide that would be available to weigh the various possibilities would assist the Commissioners in their deliberations to approve or reject the known intelligence or security staff's recommendation.

Such criteria, to us, would assist in providing more transparency as well as increasing the rigor and the consistency of the process in making those decisions. If the goal is to produce a more credible DBT, we think criteria would help, especially given that Commissioners come and go.

Mr. Chairman, GAO reported to you in 2004 that we had fairly significant concerns related to how the NRC was testing plant security. Two years later, our reaction to NRC's use of its force-on-force exercise is positive today. We saw improvements in security, like providing early detection of an attack, sufficient delay for defensive positions to be obtained, and improving capabilities of the professional guard forces to respond appropriately vastly improved over what we had seen 2 years earlier.

The initiatives that are being put in place and refined as they go we would characterize as commendable, but still represent a work in progress. A lot is riding on the quality of these tests. This type of testing is extremely important to ensure down the road that public confidence that the plants are well protected. We saw both good and not so good testing scenarios, with results that offer NRC and the industry the opportunity to make improvements.

Mr. Chairman, our bottom-line finding is that the plants' response and financial investment in the revised DBT following the September 11th attacks has truly been substantial, in the billions of dollars. And in some cases, their improvements have gone beyond what the NRC has required.

Likewise, NRC's significant staff efforts, their orders, and diligence have clearly raised the security level at the plants. Having said that, the ability to defend against an attack is essentially limited to how close the attack turns out to be to the existing DBT. It remains essential that NRC, the industry, DHS, and others remain on guard.

At our last testimony, Mr. Chairman, you may recall that we cited some somewhat challenging working relationships with the NRC to obtain information in our earlier requests from you. Today, I'd like to say that the NRC's cooperation has been excellent, and we appreciate all the senior management attention that they have given us, and we appreciate the Commissioners' support in getting the story right.

While we may continue to agree or disagree, we are impressed with the staff's desire to do a good job. It's no doubt that you are well aware that NRC faces growing challenges on many fronts, human capital issues and others, as this Nation debates the future of nuclear power. A lot is depending on the quality job that NRC has been tasked to do.

Mr. Chairman, that concludes my short remarks.

[NOTE.—The GAO March 2006 report entitled, "Nuclear Power Plants, Efforts Made to Upgrade Security, but the Nuclear Regulatory Commission's Design Basis Threat Process Should be Improved, GAO–06–388," may be found in subcommittee files.]

[The prepared statement of Mr. Wells follows:]

United States Government Accountability Office

GAO

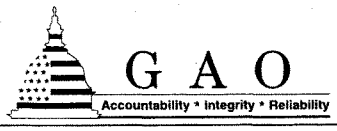
Testimony
Before the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform

For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, April 4, 2006

NUCLEAR POWER

Plants Have Upgraded Security, but the Nuclear Regulatory Commission Needs to Improve Its Process for Revising the Design Basis Threat

Statement of Jim Wells, Director
Natural Resources and Environment



GAO-06-555T

April 4, 2006

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-555T, a testimony before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

Why GAO Did This Study

The nation's commercial nuclear power plants are potential targets for terrorists seeking to cause the release of radioactive material. The Nuclear Regulatory Commission (NRC), an independent agency headed by five commissioners, regulates and oversees security at the plants. In April 2003, in response to the terrorist attacks of September 11, 2001, NRC revised the design basis threat (DBT), which describes the threat that plants must be prepared to defend against in terms of the number of attackers and their training, weapons, and tactics. NRC also restructured its program for testing security at the plants through force-on-force inspections (mock terrorist attacks). This testimony addresses the following: (1) the process NRC used to develop the April 2003 DBT for nuclear power plants, (2) the actions nuclear power plants have taken to enhance security in response to the revised DBT, and (3) NRC's efforts to strengthen the conduct of its force-on-force inspections. This testimony is based on GAO's report on security at nuclear power plants, issued on March 14, 2006 (GAO-06-388).

What GAO Recommends

In its March 2006 report, GAO recommended that NRC improve its process for making changes to the DBT and evaluate and implement measures to further strengthen its force-on-force inspection program.

www.gao.gov/cgi-bin/getrpt?GAO-06-555T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Jim Wells at (202) 512-3841 or wellsj@gao.gov.

NUCLEAR POWER

Plants Have Upgraded Security, but the Nuclear Regulatory Commission Needs to Improve Its Process for Revising the Design Basis Threat

What GAO Found

NRC revised the DBT for nuclear power plants using a process that was generally logical and well-defined. Specifically, trained threat assessment staff made recommendations for changes based on an analysis of demonstrated terrorist capabilities. The resulting DBT requires plants to defend against a larger terrorist threat, including a larger number of attackers, a refined and expanded list of weapons, and an increase in the maximum size of a vehicle bomb. Key elements of the revised DBT, such as the number of attackers, generally correspond to the NRC threat assessment staff's original recommendations, but other important elements do not. For example, the NRC staff made changes to some recommendations after obtaining feedback from stakeholders, including the nuclear industry, which objected to certain proposed changes, such as the inclusion of certain weapons. NRC officials said the changes resulted from further analysis of intelligence information. Nevertheless, GAO found that the process used to obtain stakeholder feedback created the appearance that changes were made based on what the industry considered reasonable and feasible to defend against rather than on what an assessment of the terrorist threat called for.

Nuclear power plants made substantial security improvements in response to the September 11, 2001, attacks and the revised DBT, including security barriers and detection equipment, new protective strategies, and additional security officers. It is too early, however, to conclude that all sites are capable of defending against the DBT because, as of March 30, 2006, NRC had conducted force-on-force inspections at 27, or less than half, of the 65 nuclear power plant sites.

NRC has improved its force-on-force inspections—for example, by conducting inspections more frequently at each site. Nevertheless, in observing three inspections and discussing the program with NRC, GAO noted potential issues in the inspections that warrant NRC's continued attention. For example, a lapse in the protection of information about the planned scenario for a mock attack GAO observed may have given the plant's security officers knowledge that allowed them to perform better than they otherwise would have. A classified version of GAO's report provides additional details about the DBT and security at nuclear power plants.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our recent work on security of the nation's 103 operating commercial nuclear power plants, located at 65 sites in 31 states. My testimony today is based on our report being released today, entitled *Nuclear Power Plants: Efforts Made to Upgrade Security, but the Nuclear Regulatory Commission's Design Basis Threat Process Should Be Improved* (GAO-06-388).[1]

As you know, nuclear power plants were among the targets considered in the original plan for the September 11, 2001, terrorist attacks. Furthermore, according to the Nuclear Regulatory Commission (NRC), which regulates and oversees the safe operation and security of nuclear power plants, there continues to be a general credible threat of a terrorist attack on the nation's commercial nuclear power plants, in particular by al Qaeda and like-minded Islamic terrorist groups. Such an attack could cause a release of radioactive material and endanger public health and safety through exposure to an elevated level of radiation.

To defend against a potential terrorist attack, NRC issues and enforces security-related regulations and orders, and nuclear power plant licensees implement security measures to meet NRC requirements. In particular, NRC formulates a design basis threat (DBT)—the threat that plants must defend against—and tests plants' ability to defend against the DBT. The DBT characterizes the elements of a potential attack, including the number of attackers, their training, and the weapons and tactics they are capable of employing. NRC periodically reviews the potential terrorist threat to determine whether to make changes to the DBT. Most recently, NRC revised the DBT in April 2003 in response to the September 11 terrorist attacks. After revising the DBT, NRC required nuclear power plant sites to submit new security plans by April 29, 2004, for its review and approval and to implement the security described in their new plans by October 29, 2004. In November 2004, NRC began using its force-on-force inspection program to test sites' ability to defend against the revised

[1]We also prepared a classified version of our report, which includes additional details about the DBT and security at nuclear power plants that NRC does not release to the public. For more information on NRC's oversight of security at nuclear power plants, see GAO, *Nuclear Regulatory Commission: Preliminary Observations on Efforts to Improve Security at Nuclear Power Plants*, GAO-04-1064T (Washington, D.C.: Sept. 14, 2004); and *Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened*, GAO-03-752 (Washington, D.C.: Sept. 4, 2003).

DBT. This program employs mock terrorist attacks as the principal means to test the sites' security.

The DBT does not represent the maximum size and capability of a terrorist attack that is possible but, rather, NRC's assessment of the threat that the nuclear power plants must at all times be prepared to defend against "to ensure adequate protection of public health and safety." Furthermore, NRC regulations do not require nuclear power plants to protect against attacks by an "enemy of the United States," whether a foreign government or other person.[2] NRC originally included this provision in its regulations in 1967 (prior to issuing the first DBT for nuclear power plants). According to NRC officials, the provision was intended to address the possibility that Cuba might launch an attack on a nuclear power plant in Florida. In revising the DBT in April 2003, NRC did not use this provision to exempt plants from defending against terrorist groups such as al Qaeda but, rather, stated that a private security force (such as at a nuclear power plant) cannot reasonably be expected to defend against all threats—for example, airborne attacks. Importantly, NRC works with other federal agencies to coordinate an integrated response to a terrorist threat or attack on a nuclear power plant.

Our March 2006 report examined (1) the process NRC used to develop the April 2003 DBT for nuclear power plants, (2) the actions nuclear power plants have taken to enhance security in response to the revised DBT, and (3) NRC's efforts to strengthen the conduct of its force-on-force inspections. For the report, we reviewed documents detailing the process NRC used to revise the DBT and interviewed the NRC commissioners and staff. We also visited four nuclear power plant sites (one in each of the four NRC regions) to observe the security enhancements that sites made to address the revised DBT, and we reviewed a sample of NRC's baseline and force-on-force inspection reports. GAO staff with security expertise accompanied us on our visits in order to assist in our review of the sites' security strategies. Finally, we observed a total of three force-on-force inspections at two other sites. We performed our work from November 2004 through January 2006 in accordance with generally accepted government auditing standards.

[2]10 C.F.R. § 50.13.

Summary

NRC revised the DBT for nuclear power plants using a process that was generally logical and well-defined. Specifically, trained threat assessment staff made recommendations for changes based on an analysis of demonstrated terrorist capabilities. To enhance the predictability and consistency of its assessments and its recommendations to the NRC commissioners for changes to the DBT, the NRC threat assessment staff developed and used a comprehensive screening tool to analyze intelligence information and to evaluate particular terrorist capabilities, or "adversary characteristics," for inclusion in the DBT. The resulting DBT requires plants to defend against a larger terrorist threat, including a larger number of attackers, a refined and expanded list of weapons, and an increase in the maximum size of a vehicle bomb. The revised DBT generally, but not always, corresponded to the original recommendations of the threat assessment staff. For example, the maximum number of attackers in the revised DBT is based, in part, on the staff's analysis of the size of terrorist cells worldwide. However, for other important elements of the DBT, such as the weapons that attackers could use against a plant, the final version of the revised DBT does not correspond to the staff's original recommendations. We identified the following two principal reasons for these differences:

- First, the threat assessment staff made changes to its initial recommendations after obtaining feedback from stakeholders, including the nuclear industry, on a draft of the DBT. A number of the changes reflected industry objections to the draft. For example, following meetings with industry, the staff decided not to recommend including certain weapons in the list of adversary characteristics that nuclear power plants should be prepared to defend against. In its comments, the industry had pressed for NRC to remove such adversary characteristics from the draft DBT. The industry considered them to be prohibitively expensive to defend against or to be representative of an enemy of the United States, which is the responsibility of the government, rather than the industry, to defend against. NRC officials told us the changes resulted from further analysis of the intelligence data and the reasonableness of required defensive measures rather than the industry objections. Nevertheless, in our view, this situation created the appearance that changes were made based on what industry considered reasonable and feasible to defend against, rather than an assessment of the terrorist threat.

- Second, in deciding on the revised DBT, the commissioners largely supported the staff's recommendations but also made some significant changes. These changes reflected their policy judgments on what is reasonable for a private security force to defend against. However, the commissioners did not identify explicit criteria for what is and what is not

reasonable for a private security force to defend against, such as the cost of defending against particular adversary characteristics. For example, the commissioners decided against including two weapons that the threat assessment staff had concluded could plausibly be used against a U.S. nuclear power plant. Furthermore, instead of providing a reason for its decision to remove these weapons, the commission's voting record showed that individual commissioners used differing criteria and emphasized different factors, such as cost or practicality of defensive measures. We believe the absence of reviewable criteria reduced the transparency of the decision-making process. The absence of criteria also potentially reduced the rigor of the decision-making process.

Licensees of nuclear power plants have made substantial changes to their security in response to the September 11, 2001, attacks and the 2003 revisions to the DBT. At the sites we visited, these actions included, for example, adding security barriers and detection equipment, implementing new protective strategies, enhancing access control, and hiring additional security officers. In some cases, the sites went beyond what NRC required. For example, one site added electronic intrusion detection equipment to its outer perimeter, which was not required. According to NRC, other sites implemented security enhancements similar to what we saw at the sites we visited. Despite these considerable efforts, it is too early to conclude that all sites are capable of defending against the DBT because, as of March 30, 2006, NRC had conducted force-on-force inspections at 27, or less than half, of the 65 sites. According to NRC, sites have generally performed well during force-on-force inspections, and the results of baseline inspections show that sites have generally complied with their security plans. However, a number of sites have experienced problems and have not always met security requirements. Most notably, we observed a force-on-force inspection at a site in which the licensee's performance at the time was at best questionable in its ability to defend against the DBT.

NRC has made a number of improvements to its force-on-force inspection program. For example, NRC is implementing a schedule to conduct the inspections more frequently at each site—every 3 years rather than every 8 years—and has instituted measures to make the inspections more realistic, such as using laser equipment to better simulate the weapons that attackers and security officers would likely employ during an actual attack on a nuclear power plant. These improvements are important because, as we noted from our observation of three force-on-force inspections and our review of NRC reports on others, the inspections have the ability to detect weaknesses in sites' protective strategies, which can then be corrected.

Nevertheless, in observing three inspections and discussing the program with NRC officials, we noted issues in the force-on-force program that warrant continued NRC attention. For example, the level of security expertise and training among controllers, who observe exercise participants to ensure the safety and effectiveness of the exercises, was inconsistent.

Our report included two recommendations to address the shortcomings in the process NRC used to revise the DBT. First, we recommended that NRC assign responsibility for obtaining feedback from the nuclear industry and other stakeholders on proposed changes to the DBT to an office within NRC other than the threat assessment section, thereby insulating the staff and mitigating the appearance of undue industry influence on the threat assessment itself. Second, we recommended that NRC develop explicit criteria to guide the commissioners in their deliberations to approve changes to the DBT. These criteria should include setting out the specific factors and how they will be weighed in deciding what is reasonable for a private guard force to defend against. In addition, we recommended that NRC continue to evaluate and implement measures to further strengthen the force-on-force inspection program. In commenting on a draft of our report, NRC commended our efforts to ensure that the report was accurate and constructive. NRC also provided additional clarifying comments pertaining to the process it used to revise the DBT for nuclear power plants. For example, NRC requested that we revise the report to explain that it made a deliberate decision to develop the revised DBT while simultaneously seeking input from stakeholders in order to expedite its response to the September 11, 2001 terrorist attacks. We revised the report accordingly.

Background

NRC is an independent agency established by the Energy Reorganization Act of 1974 to regulate the civilian use of nuclear materials. It is headed by a five-member commission, with one commission member designated by the President to serve as chairman and official spokesperson. The commission as a whole formulates policies and regulations governing nuclear reactor and materials safety and security, issues orders to licensees, and adjudicates legal matters brought before it. Security for commercial nuclear power plants is addressed by NRC's Office of Nuclear Security and Incident Response. This office develops policy on security at nuclear facilities and is the agency's security interface with the Department of Homeland Security (DHS), the intelligence and law enforcement communities, the Department of Energy (DOE), and other agencies. Within this office, the Threat Assessment Section assesses

security threats involving NRC-licensed activities and develops recommendations regarding the DBT for the commission's consideration.

The DBT for radiological sabotage applied to nuclear power plants identifies the terrorist capabilities (or "adversary characteristics") that sites are required to defend against. The adversary characteristics generally describe the components of a ground assault and include the number of attackers; the size of a vehicle bomb; and the weapons, equipment, and tactics that could be used in an attack. Other threats in the DBT include a waterborne assault and the threat of an insider. The DBT does not include the threat of an airborne attack.

Force-on-force inspections are NRC's performance-based means for testing the effectiveness of nuclear power plant security programs. These inspections are intended to demonstrate how well a nuclear power plant might defend against a real-life threat. In a force-on-force inspection, a professional team of adversaries attempts to reach specific "target sets" within a nuclear power plant that would allow them to commit radiological sabotage. These target sets represent the minimum pieces of equipment or infrastructure an attacker would need to destroy or disable in order to commit radiological sabotage that results in an elevated release of radioactive material to the environment. NRC also conducts baseline inspections at nuclear power plants. During these inspections, security inspectors examine areas such as officer training, fitness for duty, positioning and operational readiness of multiple physical and technical security components, and the controls the licensee has in place to ensure that unauthorized personnel do not gain access to the protected area. NRC's policy is to conduct a baseline inspection at each site every year, with the complete range of baseline inspection activities conducted over a 3-year cycle. For both force-on-force and baseline inspections, licensees are responsible for immediately correcting or compensating for any deficiency in which NRC concludes that security is not in accordance with the approved security plans or other security orders.

NRC's Process for Revising the DBT Was Generally Logical and Well Defined, but Some Changes Were Not Clearly Linked to an Analysis of the Terrorist Threat

The process by which NRC revised the DBT for nuclear power plants was generally logical and well defined in that trained threat assessment staff made recommendations for changes based on an analysis of demonstrated terrorist capabilities. The NRC commissioners evaluated the recommendations and considered whether the proposed changes constituted characteristics representative of an enemy of the United States, or were otherwise not reasonable for a private security force to defend against. However, while the final version of the revised DBT generally corresponded to the original recommendations of the threat assessment staff, some elements did not, which raised questions about the extent to which the revised DBT represents the terrorist threat.

NRC's Process for Revising Its DBT Was Generally Logical and Well Defined

NRC made its 2003 revisions to the DBT for nuclear power plants using a process that the agency has had in place since issuing the first DBT in the late 1970s. In this process, NRC staff trained in threat assessment use reports and secure databases provided by the intelligence community to monitor information on terrorist activities worldwide. (NRC does not directly gather intelligence information but rather receives intelligence from other agencies that it uses to formulate the DBT for nuclear power plants.) The staff analyze this information both to identify specific references to nuclear power plants and to determine what capabilities terrorists have acquired and how they might use those capabilities to attack nuclear power plants in the United States. The staff normally summarize applicable intelligence information and any recommendations for changes to the DBT in semiannual reports to the NRC commissioners on the threat environment.

In 1999, the NRC staff began developing a set of criteria—the adversary characteristics screening process—to decide whether to recommend particular adversary characteristics for inclusion in the DBT and to enhance the predictability and consistency of their recommendations. The staff use initial screening criteria to exclude from further consideration certain adversary characteristics, such as those that would more likely be used by a foreign military than by a terrorist group. For adversary characteristics that pass the initial round of screening, the threat assessment staff apply additional screening factors, such as the type of terrorist group that demonstrated the characteristic. For example, the staff consider whether an adversary characteristic has been demonstrated by transnational or terrorist groups operating in the United States, or by terrorist groups that operate only in foreign countries. Finally, on the basis of their analysis and interaction with intelligence and other agencies, the staff decide whether to recommend that the commission include the

adversary characteristics in the DBT for nuclear power plants. NRC's Office of Nuclear Security and Incident Response, which includes the Threat Assessment Section, reviews and endorses the threat assessment staff's analysis and recommendations.

Terrorist attacks have generally occurred outside the United States, and intelligence information specific to nuclear power plants is very limited. As a result, one of the NRC threat assessment staff's major challenges has been to decide how to apply this limited information to nuclear power plants in the United States. For example, one of the key elements in the revised DBT, the number of attackers, is based on NRC's analysis of the group size of previous terrorist attacks worldwide. According to NRC threat assessment staff, the number of attackers in the revised DBT falls within the range of most known terrorist cells worldwide.[3] NRC staff recommendations regarding other adversary characteristics also reflected the staff's interpretation of intelligence information. For example, the staff considered a range of sizes for increasing the vehicle bomb in the revised DBT and ultimately recommended a size that was based on an analysis of previous terrorist attacks using vehicle bombs. Intelligence and law enforcement officials we spoke with did not have information contradicting NRC's interpretation regarding the number of attackers or other parts of the NRC DBT but did point to the uncertainty regarding the size of potential attacks and the relative lack of intelligence on the terrorist threat to nuclear power plants.

In addition to analyzing intelligence information, NRC monitored and exchanged information with DOE, which also has a DBT for comparable facilities that process or store radiological materials and are, therefore, potential targets for radiological sabotage.[4] However, while certain aspects of the two agencies' DBTs for radiological sabotage are similar, NRC generally established less rigorous requirements than DOE— for example, with regard to the types of equipment that could be used in an attack. The DOE DBT includes a number of weapons not included in the NRC DBT. Inclusion of such weapons in the NRC DBT for nuclear power plants

[3]In this report, "terrorist cell" refers only to terrorists who participate in an attack, not those who support but do not participate in an attack.

[4]For further information on the DOE DBT, see GAO, *Nuclear Security: DOE's Office of the Under Secretary for Energy, Science and Environment Needs to Take Prompt, Coordinated Action to Meet the New Design Basis Threat*, GAO-05-611 (Washington, D.C.: July 15, 2005); and *Nuclear Security: DOE Needs to Resolve Significant Issues before It Fully Meets the New Design Basis Threat*, GAO-04-623 (Washington, D.C.: Apr. 27, 2004).

would have required plants to take substantial additional security measures. Furthermore, DOE included other capabilities in its DBT that are not included in the NRC DBT. Despite these differences, both agencies used similar intelligence information to derive key aspects of their DBTs. For example, both DOE and NRC based the number of attackers on intelligence on the size of terrorist cells, and DOE officials told us they used intelligence similar to NRC's to derive the number of attackers. Likewise, DOE and NRC officials provided us with similar analyses of intelligence information on previous terrorist attacks using vehicle bombs. DOE and NRC officials also told us that most vehicle bombs used in terrorist attacks are smaller than the size of the vehicle bomb in NRC's revised DBT.

Changes to the Threat Assessment Staff's Initial Recommendations Were Not Clearly Linked to an Analysis of the Terrorist Threat

While NRC followed a generally logical and well-defined process to revise the DBT for nuclear power plants, two aspects of the process raised a fundamental question—the extent to which the DBT represents the terrorist threat as indicated by intelligence data compared with the extent to which it represents the threat that NRC considers reasonable for the plants to defend against. These two aspects were (1) the process NRC used to obtain stakeholder feedback on a draft of the DBT and (2) changes made by the commissioners to the NRC staff's recommended DBT.

With regard to the first aspect, the process NRC used to obtain feedback from stakeholders, including the nuclear industry, created the appearance of industry influence on the threat assessment regarding the characteristics of an attack. NRC staff sent a draft DBT to stakeholders in January 2003, held a series of meetings with them to obtain their comments, and received written comments. NRC specifically sought and received feedback from the nuclear industry on what is reasonable for a private security force to defend against and the cost of and time frame for implementing security measures to defend against specific adversary characteristics. During this same period, the threat assessment staff continued to analyze intelligence information and modify the draft DBT.

In its written comments on the January 2003 draft DBT, the Nuclear Energy Institute (NEI), which represents the nuclear power industry, objected to a number of the adversary characteristics the NRC staff had included. Subsequently, the NRC staff made changes to the draft DBT,

which they then submitted to the NRC commissioners.[5] The changes made by the NRC staff—in particular, the size of the vehicle bomb and list of weapons that could be used in an attack—reflected some (but not all) of NEI's objections. For example, NEI wrote that some sites would not be able to protect against the size of the vehicle bomb proposed by NRC because of insufficient land for installation of vehicle barrier systems at a necessary distance. Instead, NEI agreed that it would be reasonable to protect against a smaller vehicle bomb. Similarly, NEI argued against the inclusion of certain weapons because of the cost of protecting against the weapons. NEI wrote that such weapons (as well as the vehicle bomb size initially proposed by the NRC staff) would be indicative of an enemy of the United States, which sites are not required to protect against under NRC regulations. In its final recommendations to the commissioners, the NRC staff reduced the size of the vehicle bomb to the amount NEI had proposed and removed a number of weapons NEI had objected to. On the other hand, NRC did not make changes that reflected all of the industry's objections. For example, NRC staff did not remove one particular weapon NEI had objected to, which, according to NRC's analysis, has been a staple in the terrorist arsenal since the 1970s and has been used extensively worldwide.

With regard to the commissioners' review and approval of the NRC staff's recommendations, the commissioners largely supported the staff's recommendations but also made some significant changes that reflected policy judgments. Specifically, the commissioners considered whether any of the recommended changes to the DBT constituted characteristics representative of an enemy of the United States, which sites are not required to protect against under NRC regulations. In approving the revised DBT, the commission stated that nuclear power plants' civilian security forces cannot reasonably be expected to defend against all threats, and that defense against certain threats (such as an airborne attack) is the primary responsibility of the federal government, in coordination with state and local law enforcement officials. Based on such considerations, the commission voted to remove two weapons the NRC staff had recommended for inclusion in the revised DBT based on its threat assessment. However, the document summarizing the commission's decision to approve the revised DBT did not provide a reason for excluding these weapons. For example, the commission did not indicate

[5]The NRC staff submitted their final draft DBT to the commissioners for their review and approval in April 2003, together with a summary of stakeholder comments.

whether its decision was based on criteria, such as the cost for nuclear power plants to defend against an adversary characteristic or the efforts of local, state, and federal agencies to address particular threats. In our view, the lack of such criteria reduced the transparency of the commission's decisions to make changes to the threat assessment staff's recommendations.

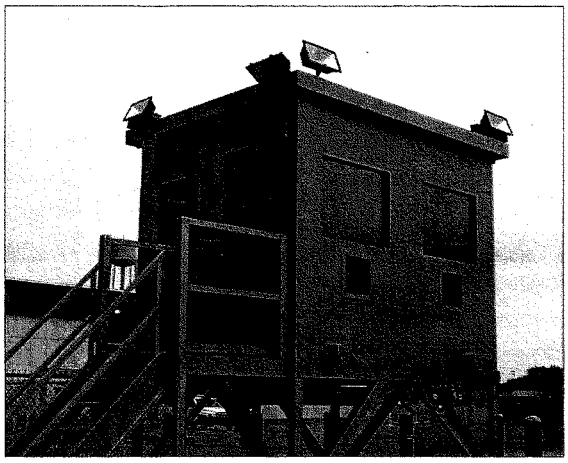
Nuclear Power Plants Made Substantial Changes to Their Security to Address the Revised DBT, but NRC Inspections Have Uncovered Problems

The four nuclear power plant sites we visited made substantial changes in response to the revised DBT, including measures to detect, delay, and respond to the increased number of attackers and to address the increased vehicle bomb size. These security enhancements were in addition to other measures licensees implemented—such as stricter requirements for obtaining physical access to nuclear power plants—in response to a series of security orders NRC issued after September 11, 2001. According to NEI, as of June 2004, the cost of security enhancements made since September 11, 2001, for all sites amounts to over $1.2 billion.

To enhance their detection capabilities, the four sites we visited installed additional cameras throughout different areas of the sites and instituted random patrols in the owner-controlled areas.[6] Furthermore, the sites we visited installed a variety of devices designed to delay attackers and allow security officers more time to respond to their posts and fire upon attackers. The sites generally installed these delay devices throughout the protected areas as well as inside the reactor and other buildings. Sites also enhanced their ability to respond to an attack by constructing bullet-resistant structures at various locations in the protected area or within buildings, increasing the minimum number of security officers defending the sites at all times, and expanding the amount of training provided to them. (See fig. 1 for an example of a bullet-resistant structure.) According to NRC, other sites took comparable actions to defend against the revised DBT.

[6]The owner-controlled area refers to the land and buildings within the site boundary that the owner can limit or allow access to for any reason. The protected area is within the owner-controlled area and requires a higher level of access control. The vital area contains the sites' vital equipment, the destruction of which could directly or indirectly endanger public health and safety through exposure to radiation.

Figure 1: Example of a Bullet-Resistant Structure



Source: Nuclear Regulatory Commission.

In addition to adding measures designed to detect, delay, and respond to an attack, the licensees at the four sites we visited installed new vehicle barrier systems to defend against the larger vehicle bomb in the revised DBT. In particular, the licensees designed comprehensive systems that included sturdy barriers to (1) prevent a potential vehicle bomb from approaching the sites and (2) channel vehicles to entrances where security officers could search them for explosives and other prohibited items. The vehicle barrier systems either completely encircled the plants (except for entrances manned by armed security officers) or formed a continuous barrier in combination with natural or manmade terrain features, such as bodies of water or trenches, that would prevent a vehicle from approaching the sites.

In general, the four sites we visited all implemented a "defense-in-depth" strategy, with multiple layers of security systems that attackers would have to defeat before reaching vital areas or equipment and destroying or disabling systems sufficient to cause an elevated release of radiation off

site. The sites varied in how they implemented these measures, primarily depending on site-specific characteristics such as topography and on the degree to which they planned to interdict attackers within the owner-controlled area and far from the sites' vital area, as opposed to inside the protected area but before they could reach the vital equipment. For example, one site with a predominantly external strategy installed an intrusion detection system in the owner-controlled area so that security officers would be able to identify intruders as early as possible. The site was able to install such a system because of the large amount of open, unobstructed space in the owner-controlled area. In contrast, security managers at another site we visited described a protective strategy that combined elements of an external strategy and an internal strategy. For example, the site identified "choke points"—locations attackers would need to pass before reaching their targets—inside the protected area and installed bullet-resistant structures at the choke points where officers would be waiting to interdict the attackers. NRC officials told us that licensees have the freedom to design their protective strategies to accommodate site-specific conditions, so long as the strategies satisfy NRC requirements and prove successful in a force-on-force inspection.

In addition to the security enhancements we observed, security managers at each site described ways in which they had exceeded NRC requirements and changes they plan to make as they continue to improve their protective strategies. For example, security managers at three of the sites we visited told us the number of security officers on duty at any one shift exceeded the minimum number of security officers that NRC requires be dedicated to responding to attacks. Similarly, in at least some areas of the sites, the new vehicle barrier systems were farther from the reactors and other vital equipment than necessary to protect the sites against the size of vehicle bomb in the revised DBT.

Despite the substantial security improvements we observed at the four sites we visited, it is too early to conclude, either from NRC's force-on-force or baseline inspections, that all nuclear power plant sites are capable of defending against the revised DBT for the following two reasons:

- First, as of March 30, 2006, NRC had completed force-on-force inspections at 27 of the 65 sites, and it is not planning to complete force-on-force inspections at all sites until 2007, in accordance with its 3-year schedule. NRC officials told us that plants have generally performed well during force-on-force inspections. However, we observed a force-on-force inspection at one site in which the site's ability to defend against the DBT was at best questionable. The site's security measures appeared

impressive and were similar to those we observed at other sites. Nevertheless, some or all of the attackers were able to enter the protected area in each of the three exercise scenarios. Furthermore, attackers made it to the targets in two of the scenarios, although the outcomes of the two scenarios were called into question by uncertainties regarding whether the attackers had actually been neutralized before reaching the targets. As a result, NRC decided to conduct another force-on-force inspection at the site, which we also observed. The site made substantial additional security improvements—at a cost of $37 million, according to the licensee—and NRC concluded after the second force-on-force inspection that the site had adequately defended against a DBT-style attack.

- Second, we noted from our review of 18 baseline inspection reports and 9 force-on-force inspection reports that sites have encountered a range of problems in meeting NRC's security requirements. NRC officials told us that all sites have implemented all of the security measures described in their new plans submitted in response to the revised DBT. However, 12 of the 18 baseline inspection reports and 4 of the 9 force-on-force inspection reports we reviewed identified problems or items needing correction. For example, during two different baseline inspections, NRC found (1) an intrusion detection system in which multiple alarms were not functioning properly, making the entire intrusion detection system inoperable, according to the site, and (2) three examples of failure to properly search personnel entering the protected area, which NRC concluded could reduce the overall effectiveness of the protective strategy by allowing the uncontrolled introduction of weapons or explosives into the protected area. According to NRC, the licensees at these two sites, as well as at the other sites where NRC inspection reports noted other problems, took immediate corrective actions.

NRC Has Significantly Improved the Force-on-Force Inspection Program, but Challenges Remain

NRC has made a number of improvements to the force-on-force inspection program, several of which address recommendations we made in our September 2003 report on NRC's oversight of security at commercial nuclear power plants. We had made our recommendations when NRC was restructuring the force-on-force program to provide a more rigorous test of security at the sites in accordance with the DBT, which was also under revision. For example, we recommended that NRC conduct the inspections more frequently at each site, use laser equipment to better simulate attackers' and security officers' weapons, and require the inspections to make use of the full terrorist capabilities stated in the DBT. Actions NRC has taken that satisfy these recommendations include conducting the exercises more frequently at each site (every 3 years rather than every 8 years), and NRC so far is on track to complete the first round

of force-on-force inspections on schedule, by 2007. Furthermore, NRC is using laser equipment to simulate weapons, and the attackers in the force-on-force exercise inspections that we observed used key adversary characteristics of the revised DBT, including the number of attackers, a vehicle bomb, a passive insider, and explosives.

Nevertheless, we identified issues in the force-on-force inspection program that could affect the quality of the inspections and that continue to warrant NRC's attention. For example, the level of security expertise and training among controllers—individuals provided by the licensee who observe each security officer and attacker to ensure the safety and effectiveness of the exercise—varied in the force-on-force inspections we observed. One site used personnel with security backgrounds while another site used plant employees who did not have security-related backgrounds but who volunteered to help. In its force-on-force inspection report for this latter site, NRC concluded that the level of controller training contributed to the uncertain outcome of the force-on-force exercises, which resulted in NRC's conducting a second force-on-force inspection at the site.

Furthermore, we noted that the force-on-force exercises end when a site's security force successfully stops an attack. Consequently, at sites that successfully defeat the mock adversary force early in the exercise scenario, NRC does not have an opportunity to observe the performance of sites' internal security—that is, the strategies sites would use to defeat attackers inside the vital area. When we raised this issue, NRC officials appeared to recognize the benefit of designing the force-on-force inspections to test sites' internal security strategies but said that doing so would require further consideration of how to implement changes to the force-on-force inspections. Based on our observations of three force-on-force inspections, other areas where NRC may be able to make further improvements included the following:

- ensuring the proper use of laser equipment;
- varying the timing of inspection activities, such as the starting times of the mock attacks, in order to minimize the artificiality of the inspections;
- ensuring the protection of information about the planned scenarios for the mock attacks so that security officers do not obtain knowledge that would allow them to perform better than they otherwise would; and

- providing complete feedback to licensees on NRC inspectors' observations on the results of the force-on-force exercises.

Mr. Chairman, this completes my prepared statement. I would be happy to respond to any questions you or the other Members of the Subcommittee may have at this time.

GAO Contact and Staff Acknowledgments

For further information about this testimony, please contact me at (202) 512-3841 (or at wellsj@gao.gov). Raymond H. Smith, Jr. (Assistant Director), Joseph H. Cook, Carol Herrnstadt Shulman, and Michelle K. Treistman made key contributions to this testimony.

GAO's Mission	The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."
Order by Mail or Phone	The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to: U.S. Government Accountability Office 441 G Street NW, Room LM Washington, D.C. 20548 To order by Phone: Voice: (202) 512-6000 TDD: (202) 512-2537 Fax: (202) 512-6061
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, D.C. 20548
Public Affairs	Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, D.C. 20548

Mr. SHAYS. Thank you, Mr. Wells.

I think that it is important that you point out, given that you weren't satisfied with the relationship before, that you have made it very clear that you are pleased with that relationship. And that is duly noted and appreciated.

I thank you. I thank the Commissioners for that. That is the way it should be.

Mr. WELLS. Thank you.

Mr. SHAYS. Mr. Diaz.

STATEMENT OF NILS J. DIAZ

Mr. DIAZ. Mr. Chairman, it's a pleasure to be before you today with my fellow Commissioners; Commissioner McGaffigan, Commissioner Merrifield.

Commissioner Jaczko and Commissioner Lyons are not here for different reasons.

Mr. SHAYS. They wouldn't fit at this table. [Laughter.]

Mr. DIAZ. I think they knew that. But they do send their regrets.

We do appreciate the opportunity to discuss the efforts and accomplishments of the U.S. Nuclear Regulatory Commission and its licensees to improve safety and security at nuclear power plants. Testimony today will focus on the Government Accountability Office's recent report, and we'll also provide an update on the status of nuclear power plant security.

The Commission appreciates the efforts of GAO in reviewing this important topic; the care taken to ensure that the report is comprehensive, up to date, and accurate; and the consideration given to NRC's comments. We believe GAO's input and its criticism are constructive, and we are taking their recommendations very seriously.

Mr. Chairman, safety, security, and emergency preparedness at nuclear power plants are synergistically improving. Our organization and the licensees' organization have changed to respond to the post September 11th world and did change rapidly.

The safety and security framework for reactors and materials is in place. It's tested and being improved commensurate with the September 11th threat and potential consequences. The agency's security and research program were major contributors to the security assessments that were done and the improvements made.

These programs focused on defining the vulnerabilities and security needs and then were integrated with operational safety and licensing priorities, leveraging resources and expertise with our Federal partners and national laboratories.

We continue to manage and prioritize resources, including our human resources needs, investing in the present and in the near future, while exercising appropriate fiscal restraint.

In its recent report, GAO recommended that NRC improve its process for making changes to the DBT. Additionally, GAO recommended that the NRC should separate the responsibility of receiving and considering external stakeholder feedback from the process of developing the specific threat characteristics in the DBT. It is important to consider those recommendations in the proper context.

On February 25, 2002, the NRC supplemented its security regulations through orders to power reactor licensees imposing interim compensatory measures informed by information received from law enforcement and intelligence agencies. The orders were based on a review which included land, water-borne, and aircraft threats, for estimating damage, enhancing deterrence, prevention and mitigation, and reducing potential consequences to the public.

These measures required power reactor licensees to enhance security and improve the capabilities to respond to a terrorist attack, effective August 31, 2002. These orders constituted a de facto supplement to the DBT by adding appropriate security enhancements that the NRC deemed necessary in light of the heightened threat environment and were arrived at with no industry input.

The interim compensatory measures provided a significant foundation for the subsequent orders. These enhancements to security included significantly increasing the numbers of dedicated security guards with threat response duties, increased vehicle standoff distances, addition of water-borne threats, and improved coordination with law enforcement and intelligence communities, as well as strengthened safety-related mitigation procedures and strategies and enhanced background investigation.

Furthermore, on April 29, 2003, the NRC, after soliciting and receiving comments from appropriate Federal, State, and industry stakeholders, issued orders supplementing the DBTs and provided additional details regarding specific adversary characteristics against which power reactors need to protect.

While the specifics of these changes are sensitive, the supplements to the existing threat resulted in enhancements such as increased patrols, augmented security forces and capabilities, additional security posts, additional physical barriers, vehicle checks at greater standoff distances, enhanced coordination with law enforcement and military authorities, augmented security and emergency response training, equipment, and communications, and more restrictive site access control for personnel, including expanded, expedited, more thorough background checks and enforceable work hour limits and training for security force personnel.

All these orders required implementation by October 29, 2004, and have been inspected for compliance.

The NRC conducts security oversight to ensure compliance with its requirements, including baseline inspection programs and force-on-force exercises. The NRC conducted force-on-force testing at nuclear power plants since well before the events of September 11th and has since enhanced the program significantly.

The force-on-force program is a performance-based NRC program to physically test and evaluate the site's defensive strategies concerning the DBT. The GAO report recognized its value to the continual improvement of security at NRC facilities. The NRC continues to enhance the programs through the integration of lessons learned from previous exercises.

Since September 11th, we have conducted force-on-force exercises, including the pilots and the extended pilots at 53 of the 64 reactor sites, 26 after the full program was started and 27 in the pilot program and the enhanced pilot program.

Currently, the NRC is also implementing key provisions of the Energy Policy Act of 2005 that will help augment the oversight of security for nuclear facilities and materials. For example, the act authorizes the possession and use of certain firearms by security personnel. The Commission is very pleased that many long-sought security-related pieces of legislation were included in the Energy Policy Act, and we thank the Congress for its support.

In its recent report, GAO recommended that the Commission develop explicit criteria for defining what is and is not reasonable for a private security force to defend against. The Commissioners' decision regarding final approval of a supplemental DBT were not arbitrary. The Commissioners' deliberations and decisionmakings were comprehensive, thorough, risk-informed, and resulted in effective enhancements of defensive capabilities of nuclear power plants.

While additional delineations of relevant considerations might be useful in some circumstances, reasoned judgment within this and other areas of the Commission's statutory decisionmaking authority does not require and, in fact, could be unduly restricted by detailed prescriptive criteria. Moreover, overly detailed prescriptive criteria could be detrimental to good regulatory decisionmaking.

GAO's second recommendation focused on the process used by the Commission to obtain external stakeholder input while developing the supplemented DBT in 2003. Again, we believe we needed to act promptly, but deliberately. Issuance of orders is not and should not be routine, but it was expeditious at the time.

We agree with GAO that separation of the threat assessment process and the establishment of the DBT characteristics should be maintained. Now that the NRC has returned to our normal DBT review process, wherein we sequentially develop a revision to the DBT, then seek external stakeholder input, we have fully addressed GAO's concern.

Mr. Chairman, the Nuclear Regulatory Commission acted promptly and effectively to integrate increased security at nuclear power plants with safety and emergency preparedness. We continue to strengthen our partnership with Federal, State, and local authorities to provide and integrate the response to potential threats of nuclear power plants.

Our oversight confirms that licensees have implemented the requirements and have adequate security, safety, and preparedness capability to ensure protection of the American people.

We will be pleased to answer the questions of the subcommittee.

[The prepared statement of Mr. Diaz follows:]

STATEMENT SUBMITTED

BY THE

UNITED STATES NUCLEAR REGULATORY COMMISSION

TO THE

COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND

INTERNATIONAL RELATIONS

UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

NUCLEAR SECURITY

PRESENTED BY

NILS J. DIAZ

CHAIRMAN

SUBMITTED: APRIL 4, 2006

Introduction

Mr. Chairman and Members of the Subcommittee, it is a pleasure to appear before you today to discuss the efforts and accomplishments by the U.S. Nuclear Regulatory Commission (NRC) and its licensees with respect to security at nuclear power plants. The NRC appreciated the opportunity to testify before this Subcommittee on September 14, 2004, regarding nuclear power plant security. The testimony today provides an update of our prior testimony, with a special focus on the Government Accountability Office's (GAO) recent report, GAO-06-388, "Nuclear Power Plants: Efforts Made to Upgrade Security, but the Nuclear Regulatory Commission's Design Basis Threat Process Should Be Improved."

Overview

The NRC's mission is to regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, to promote the common defense and security and to protect the environment. On behalf of the entire U.S. Nuclear Regulatory Commission, I am pleased to report that the NRC continues to discharge its responsibilities well, ensuring that the commercial use of radioactive and nuclear materials including nuclear power plants remain safe and secure.

As we have previously reported, nuclear power plants have built-in features that strengthen their ability to withstand externally initiated events. They were designed to withstand catastrophic events including, but not limited to, fire, flood, earthquakes, and tornadoes. These plants were also designed to employ a defense-in-depth strategy, with redundant safety

systems and are operated and protected by highly trained staff. Multiple barriers protect the nuclear fuel and the reactor and help prevent or mitigate off-site releases of radioactive materials. The original design features of the reactor facilities, as well as subsequent enhancements, provide substantial inherent protection against a malevolent attack. The NRC and its licensees continue to develop additional protective strategies necessary to complement the facilities capabilities to prevent, detect, and mitigate potential events.

Security at nuclear facilities across the country has long been the subject of NRC, and its predecessor, the Atomic Energy Commission (AEC), regulatory oversight. These security programs are designed, implemented and verified to defend against violent assaults by well-armed, well-trained adversaries. The sites employ sophisticated surveillance equipment, stringent access controls, physical barriers, and well-qualified and trained armed response forces to implement a site-specific defense strategy. Integrated with State, local and Federal law enforcement, we believe the sites are the best protected and tested commercial facilities in the Nation.

Summary of Security Performance

The NRC has a long history of ensuring the safety and security of civilian uses of nuclear power and materials. The NRC's process for reviewing and updating security requirements is based on decades of assessments and lessons learned. These have been integrated into a comprehensive protective scheme of regulatory requirements that are fully executed by our licensees; these requirements to be assessed, and when necessary enhanced.

4

Security, while clearly receiving added focus following the events of September 11, has long been an intrinsic component of NRC's regulatory framework and was originally addressed in the Atomic Energy Act of 1954, as amended. This Act created the AEC and outlined the essential requirements of a regulatory program to oversee the civilian use of nuclear material. It also provided the basis for regulations designed to guard against theft or diversion of special nuclear material, which included, but was not limited to, materials used in nuclear reactors. In the decade that followed its founding, the AEC required careful maintenance of inventories of special nuclear material and that specific consideration be given to the threat of theft or diversion when considering licensing approvals and actions.

In 1974, the Energy Reorganization Act established the NRC and addressed international terrorism and the need to secure increasing numbers of nuclear facilities and increasing inventories of potentially weapons-usable material in the private sector. The Act required the NRC to review all existing safeguards and security requirements and recommend upgrades where necessary.

During this same period, a Security Agency Study was undertaken. Completed in August 1976, the study focused on the possible establishment of a Federal protective security force to provide protection at commercial power reactors. The study found that the "...creation of a Federal guard force would not result in a higher degree of guard force effectiveness than can be achieved by the use of private guards, properly trained, qualified, trained and certified by the NRC." Shortly after September 11, this issue was again raised. The NRC continues to support the concept that a private security guard force, with special emphasis on performance-based training and full accountability, is the best approach to securing our Nation's commercial nuclear facilities.

In 1977, following the completion of multiple interagency working groups and fact-finding efforts, the NRC amended its regulations to specify physical security measures for nuclear power reactors and special nuclear material . By 1979, additional concerns arose regarding arms proliferation, industrial sabotage and global terrorism. In response, the Commission issued new regulations to incorporate a range of physical security upgrades, including finalizing the DBTs. The use and review of the DBT is an ongoing process; for example, in 1994, the NRC revised the DBT for radiological sabotage to incorporate threat lessons-learned from the 1993 World Trade Center bombing, the Three Mile Island vehicular intrusion in 1993, and terrorist attacks on a variety of foreign facilities. The NRC maintains a deliberate process for reviewing current threat information on an ongoing basis. For almost three decades, the NRC's threat assessment staff has reviewed domestic and international events on a daily basis to determine significance and appropriate NRC actions. Threat assessment and security staff from NRC Headquarters and Regions are available as part of the Information Assessment Team to conduct timely coordination with licensees, law enforcement and the intelligence community to respond to potential threats.

Nuclear Power Plant Defensive Strategies

While nuclear power plants have been required for decades to maintain physical security programs, the terrorist attacks on September 11, 2001, reaffirmed the need for additional collective vigilance, the need for enhanced security, and improved emergency preparedness and incident response capabilities across the Nation's critical infrastructure. As a result, the NRC conducted a comprehensive review of licensees' security programs

and made further enhancements to security at a wide range of NRC-regulated activities and facilities.

Immediately following the September 11 attacks, the NRC placed nuclear power plants and other facilities at the highest level of alert using established procedures. On February 25, 2002, the NRC supplemented its security regulations through Orders to power reactor licensees imposing Interim Compensatory Measures, coordinating with law enforcement and intelligence agencies. These measures required power reactor licensees to enhance security and improve their capabilities to respond to a terrorist attack. These Orders constituted a de facto supplement to the DBT, by adding appropriate security enhancements that the NRC deemed necessary in light of the heightened threat environment. Many of these changes, arrived at with no industry input, were among the basis for the subsequent Orders. These enhancements to security included significantly increasing the number of dedicated security guards with threat response duties, increased vehicle standoff distances, consideration of water-borne threats, and improved coordination with law enforcement and intelligence communities, as well as strengthened safety-related mitigation procedures and strategies. Subsequently, on January 7, 2003, the NRC issued additional Orders to licensees to enhance background investigations of persons applying for and holding unescorted access to power reactor facilities.

Furthermore, on April 29, 2003, the NRC, after soliciting and receiving comments from appropriate Federal, State, and industry stakeholders, issued Orders supplementing the DBTs, providing additional details regarding specific adversary characteristics against which power reactors and Category I fuel cycle facilities (facilities that process highly enriched uranium), need to protect. While the specifics of these changes are sensitive or classified, in general these supplements to the existing threat resulted in enhancements such as increased patrols,

augmented security forces and capabilities, additional security posts, additional physical barriers, vehicle checks at greater standoff distances, enhanced coordination with law enforcement and military authorities, augmented security and emergency response training, equipment, and communication, and more restrictive site access controls for personnel, including expanded, expedited, and more thorough employee background checks. Concurrently, additional Orders required nuclear power plant licensees to impose enforceable work-hour limits on security force personnel and procedures to evaluate security force fatigue and to enhance training and qualification programs to ensure that armed security personnel are fit, properly trained, and qualified.

The NRC's process for reviewing and updating the specific attributes of the design basis threat is deliberate, thorough, and well-informed. The NRC maintains a competent and dedicated staff that routinely interacts with the intelligence community to gather and review all relevant threat information. Thus, the Commission's decisions and direction to the staff regarding supplementing the DBT, the issuance of security-related Orders, and the subsequent follow-on rulemaking are informed by a variety of sources, including input from NRC staff and external stakeholders.

The NRC conducts security inspection programs to ensure compliance with its requirements, including a baseline inspection program and force-on-force exercises. The NRC conducted force-on-force testing at nuclear power plants since well before the events of September 11 and has since enhanced the program significantly. The NRC, nuclear industry, and certain other stakeholders have leveraged technology, increased funding, and committed additional personnel toward the continual improvement of this effort. The force-on-force

exercises test a nuclear power plant's ability to meet requirements that the licensee must defend with a high degree of assurance.

The force-on-force program is a performance-based NRC program to physically test and evaluate the sites' defensive strategies concerning the DBT. The GAO report recognized its value to the continual improvement of security at NRC-regulated nuclear facilities. The NRC continues to enhance the program through the integration of lessons learned from previous exercises. Additionally, the NRC emphasizes use of advanced technology to minimize exercise artificialities, some of which have been identified in the report by GAO. The NRC concurs fully with the report's recommendation that "the NRC continue to evaluate and implement measures to further strengthen the force-on-force inspection program."

The force-on-force inspections at nuclear power plants involve significant preparation on the part of the NRC both in the weeks leading up to and during the on-site visit. NRC employs multiple mock adversary teams whose members possess comprehensive and complementary skill sets. Using proven operational security principles and state-of-the-art equipment, the teams develop, execute, and test threat scenarios through a series of exercises. As reflected in its report to the Committee, the GAO team observed a total of nine such exercises.

Safety is the NRC's first priority in the conduct of each force-on-force exercise. While every participant in the planning and execution of the exercise works to minimize the effects of necessary "artificialities", there are personnel and plant safety limits that must be maintained. Safety briefings and plant-wide notifications of the general schedule must be disclosed, and an increased presence of non-plant personnel will be evident. With that in mind, NRC staff and

other participants are not allowed to share any information with the site regarding attack methodologies or tactics that will be employed during the exercise.

GAO Recommendations from its September 14, 2004 Testimony

I would like to take this opportunity to clarify the NRC's response to previous GAO recommendations on nuclear power plant security. GAO's September 2003 report and September 2004 testimony on nuclear power plant security made certain accountability-related recommendations. The first recommendation involved requiring inspectors to conduct follow-up visits to verify that corrective actions have been taken, even when a violation does not reach the threshold for being "cited." Licensees are required to address violations through their Corrective Action Program and the NRC does complete a follow-up visit on specific categories of cited violations.

GAO also recommended collecting and sharing lessons learned among the NRC Regions and licensees. As I have mentioned, there are multiple methods for collecting and sharing information. In addition to generic communications, such as the Regulatory Issue Summaries and Information Notices, the NRC headquarters security staff conducts weekly teleconferences with Regional Security Inspectors, Deputy Regional Administrators and Regional Inspectors. The NRC fully concurs that such communication and information sharing needs to be enhanced continually and is doing so. In addition, the NRC is committed to sharing security best practices among its licensees.

The last 2004 recommendation focused on ensuring the NRC's policy of submitting the results of force-on-force exercises within 45 calendar days was followed. The NRC agrees that

reports need to be submitted in a timely manner. The NRC remains committed to improving in this area, as evidenced by a recent review indicating that of the seven most recent reports, only one went beyond the 45 day time line.

GAO Report Regarding Nuclear Power Plant Security and the DBT Revision Process

The GAO report indicates that it reviewed the NRC's documented findings from 27 baseline inspection and force-on-force reports. The findings identified by NRC were the result of good inspection practices on the part of NRC inspectors and good self-assessments by the licensees. In each case, the issue was identified and resolved. Depending on the severity of the finding, inspectors remained on-site until the licensee implemented appropriate compensatory measures. The NRC continues to inspect and licensees continue to be responsive when deficiencies are identified.

In its report, GAO recommended that "NRC improve its process for making changes to the DBT." Additionally, GAO recommended that the NRC should separate the responsibility of receiving and considering external stakeholder feedback from the process of developing the specific threat characteristics in the DBT.

With regard to improving the NRC decision-making process, GAO recommended that the Commission should develop explicit criteria for defining what is and is not reasonable for a private security force to defend against. As stated in our January 24 and February 23, 2006, letters to the GAO, the NRC rejects any implication that the Commissioners' decisions regarding final approval of the supplemented DBT were arbitrary. While additional delineation

of relevant considerations might be useful in some circumstances, reasoned judgment within this and other areas of the Commission's statutory decision-making authority does not require, and in fact could be unduly restricted, by detailed prescriptive criteria. Moreover, consistent with governing statutes, the Commission utilized an appropriate decision-making process by providing for a majority Commission position on well-documented staff papers in order for actions to proceed, and documenting individual Commissioner views and proposed modifications for consideration by other Commissioners. The Commission's statutory authority under the Atomic Energy Act and the Energy Reorganization Act, coupled with broad, cross-cutting policy considerations, regular briefings, documented staff papers, and a detailed decision-making process provide the necessary and sufficient criteria for the Commission to make informed decisions regarding the DBT. Moreover, overly-detailed, prescriptive criteria could be detrimental to good governance.

GAO's second recommendation focused on the process used by the Commission to obtain external stakeholder input while developing the supplemented DBT in 2003. The Commission unanimously decided to seek input from all cleared stakeholders on the draft supplemental DBT in January 2003. As noted above, much of the staff's proposed draft DBT derived either explicitly or implicitly from the February 25, 2002 Order on which the Commission had consulted with law enforcement and intelligence agencies. Every State with an affected licensee, every Federal law enforcement, security and intelligence agency, and each affected licensee was asked to comment on the draft within a very short comment period for expeditious deliberations and implementation. Industry input was but one factor, and not a particularly significant one, in the Commission's ultimate decision on the supplemental DBT issued on April 2003. In any case, now that the NRC has returned to our normal DBT review process, wherein

we sequentially develop a revision to the DBT then seek external stakeholder input, we believe most of GAO's concern will be alleviated regarding the appearance of undue influence by industry stakeholders.

Path Forward

As the Subcommittee may recall, in its September 2004 testimony, the NRC urged that specific legislative enhancements be enacted. Title VI of the Energy Policy Act of 2005 provides essentially all of these enhancements that collectively will provide additional protection to nuclear power plants. Provisions such as enhanced weaponry, broader fingerprinting and background checks, and criminal penalties for introduction of dangerous weapons and for sabotage of power plants were incorporated.

In addition to and consistent with Congress' legislative actions, the NRC initiated a rulemaking in which it proposed to update the DBT to reflect, among other things, the enhancements and supplementing requirements imposed in the Orders. For example, consideration of a broad range of DBT-related threat factors are explicitly included in NRC's current 10 CFR 73.1 rulemaking. Enhanced weaponry, more rigorous fingerprinting and background checks, and additional measures learned through the implementation of the post September 11 security Orders are also part of a separate 10 CFR 73.55 rulemaking.

Looking toward the future, the NRC recognizes that as the threat environment evolves, we must be positioned to respond decisively. Within the NRC, we must continue to attract and retain employees with the skill sets necessary to manage the challenge. The support of

government agencies at the Federal, State and local levels, the legislative branch, and private sector stakeholders must continue to be leveraged to ensure continued success. We are confident that the NRC has the capability and commitment to continue our successful efforts in these areas.

Summary

GAO's audit of nuclear power plant security began in 2003. In the subsequent three years, GAO, the NRC, and multiple nuclear power plant licensees have expended significant resources to provide this Subcommittee and the American public with a greater understanding of the security structure in place to protect nuclear power plants against the potential impact of a terrorist attack. Because some security requirements have been imposed by the NRC through Orders and licensees' security plans, with related safeguards or classified information, cannot be shared in a public forum without compromising security, the GAO's public report should not be considered a full and complete accounting of the state of nuclear power plant security. The sum total of classified and unclassified security requirements provide a comprehensive and appropriate defense against potential terrorist attacks. We remain confident that nuclear power plant security plans are adequate to ensure the protection of the American people from malevolent attempts to damage vital plant equipment and release hazardous radioactive materials to the environment.

We appreciate the opportunity to appear before you today and look forward to answering any questions you might have.

Mr. SHAYS. Thank you, Mr. Chairman.

And I would just note, the other Commission members, when we ask questions, just jump in as full participants here.

I would like just first to have an explanation of the 27 figure, and you give the 26 plus 27. So maybe, Mr. Wells, I would like you to respond first just so I have a sense of how you can reconcile those numbers. I know the chairman can, but how do you reconcile them?

Mr. WELLS. The numbers we used were the reports that were available based on baseline inspections and force-on-force exercises that had been conducted since the revised DBT was implemented in 2003, after October.

I believe the chairman's numbers including going back all the way to September 11th timeframe years before. Quite frankly, 2 years ago, when we looked at their old inspection program, we found a lot of problems and weren't too impressed with the rigor of that inspection. So we didn't include those numbers. We only included what they've done since, recently.

Mr. SHAYS. Would you concur that is the difference of the numbers, Mr. Diaz?

Mr. DIAZ. Not exactly, Mr. Chairman.

The 26 numbers are what we call the numbers of the force-on-force exercises that were conducted after the security plans were in place.

Mr. SHAYS. But not before the design basis threat?

Mr. DIAZ. After the design basis threat was established, we started to conduct pilot programs, which are not exactly the same as they conducted, but they were force-on-force programs.

Mr. SHAYS. Right. No, but you do agree that the 27 are basically from the design basis threat?

Mr. DIAZ. No. Yes, from the time that the full program is started.

Mr. SHAYS. Right. Right.

Mr. DIAZ. Two years before, we had been conducting——

Mr. SHAYS. So where you might have the disagreements are that what you did before, you would say is valid, Mr. Wells would question, and I would probably side more with Mr. Wells on that. I mean, the design basis threat was, it upped the ante a bit. You had to meet a stronger standard.

Mr. DIAZ. They were very close, sir. They were very close.

Mr. SHAYS. I hope they weren't close.

Mr. DIAZ. No, no. Because——

Mr. SHAYS. Don't go down that road.

Mr. DIAZ. Because the February 25, 2002, orders served as a very good baseline for the DBT. By the time the DBT was implemented or was not implemented, by the time we actually established the orders in April 2003, we commenced with a series of pilots on force-on-force that actually helped us see what was the implementation needs, what things needed to be done.

And in many ways, they did serve a very good purpose of informing the Commission of the compliance of the licensees so that there was no compliance issues. We have——

Mr. SHAYS. I am not saying it was better than nothing, but it wasn't as good as what happened after you had a design basis threat. So I am not saying it was useless. I am just saying what

the design basis threat, once you did that, you have done 27. That is the marker we are using.

Mr. MCGAFFIGAN. Mr. Chairman, I think it's more important to focus on where we agree, and Mr. Wells agrees that what we're doing today in the 27, which is exactly what Congress asked us to do in the Energy Policy Act; do 1 every 3 years at each of these sites; 22 a year. It's been a little more than a year. That's why the 27.

We are doing that. We're doing it well, and we're continuing to try to make improvements as we bring in, you know, additional ways to deal with realism. By the way, we don't do them all in the daytime. We do them at night.

Mr. SHAYS. Yes. We will talk a little more about it. But let me just say what I think is the most helpful. What is most helpful to this subcommittee is as accurate and precise information as we can get and not trying to win an argument here.

One of the values, and I appreciate the Commission understanding that it is helpful to have the GAO at the table rather than have them come separate and so on; but this isn't a debate. We are not trying to win arguments. We are just trying to know the truth, know where our strengths are, where our weaknesses are.

We are all under oath in this subcommittee because we really value real accuracy. So, I am not trying to get in any game here. I just want to know the distinctions.

So, what I am going to carry from that last question is you did 26 before you had a design basis threat. It was helpful. Your statement is that design basis, that wasn't all that different. I think there was some differences.

Mr. DIAZ. There are some differences, sir.

Mr. SHAYS. Yes.

Mr. DIAZ. There are some differences.

Mr. SHAYS. There had to have been. And I know when I am dealing with the Energy Department as it relates to the protection of their facilities, when we walk through about four of those sites, we had some very serious—this is a number of years ago—about the design basis threat. And frankly, there were some assumptions that were almost absurd, absurd in that they didn't look at what we think would be a real issue.

I don't think you are going to be faced with an attack at every site. I think you are going to be faced with an attack at one or two sites that will be so well thought out and will take years to develop. In other words, by developing, having someone in-house be part of the problem, or maybe two.

Just as an example, without talking about what your design basis threat is, there is a huge difference between two insiders and one. Assumption makes the reality of dealing with it much different.

Let me ask you what role did the industry play in helping the Commission establish the design basis threat? And let me say before you answer, it had to have some role. So don't tell me it didn't have any role. Then we have big problems. Just tell me how much a role.

Mr. DIAZ. Well, sir, the staff, first, worked with intelligence community and worked with State authorities to come up with a threat

assessment. Once that threat assessment was established, it was determined at the time that it would be more expeditious to engage those stakeholders that were cleared.

Of course, one of our principal stakeholder groups consists of the licensees, those who are going to have to implement the DBT, those who are going to have to actually manage the security forces. And at that time, the staff determined that it was appropriate to get them involved, to get feedback on what the DBT was, and they received that feedback.

However, I must say that the deliberations of the Commission were separate from that. The Commission maintains a separation with the staff, and we actually have that process in place.

The staff actually went, prepared it, and then interacted with the industry, received feedback from the industry, and then the deliberations of the Commissioners—especially these three Commissioners, which were actually there and doing the deliberation—was totally separate from the industry.

Mr. SHAYS. Wouldn't it be more logical to have established what you viewed as the design basis threat and then asked the industry to respond? And I realize that it would be behind closed doors.

But in other words, rather than their input before, wouldn't it have been almost better to have their input after?

Mr. MCGAFFIGAN. Mr. Chairman, just in terms of the process we followed, as Chairman Diaz said, in February 2002, we issued an order with no industry input, based only on law enforcement——

Mr. SHAYS. When was that, 2002?

Mr. MCGAFFIGAN. February 2002. Within 6 months after September 11th. And Chairman Diaz, as a Commissioner then, should take credit because he was the driving force behind we've got to get this out. Dick Meserve was our chairman at the time.

We put that out. No industry input. We actually had a few glitches as a result of that because some of the words were not precise, and we had to issue some clarifying guidance later in the year.

In late 2002, we had tasked the staff to come up with a DBT that could go forward. In January 2003, we took that staff document, without change, and gave it to the law enforcement, intelligence, and security agencies of the Government, to all the States that had NRC facilities in them, and to the industry for comment.

So, without industry input, we put out a draft document for comment. At that point, we got input. Twelve of the States came back and gave us input.

Mr. SHAYS. Is this for the final DBT that you——

Mr. MCGAFFIGAN. This is for the final DBT. I'm talking January 2nd or 3rd, 2003, heading toward an April decision on the final DBT.

So the process that we went through was to get as broad comment as we could from those who had clearances. So, as I said, all the States——

Mr. SHAYS. I get the picture here. I understand what you are saying.

Now let me ask you, Mr. Wells, have you seen that document that was the earlier document that they were asked to comment on?

Mr. WELLS. Yes, we have.

Mr. SHAYS. OK. Were there significant changes from that document, as you recall?

Mr. WELLS. The process, as we saw it in January 2003, the threat assessment staff, based on their assessment of intelligence, available information, recommended at least in the five major areas a level of DBT support, number of attackers, vehicle bombs, weapons, and equipment, and explosives.

In January 2003, they were also involved in getting input from the——

Mr. SHAYS. Who is "they?"

Mr. WELLS. The threat assessment staff were also involved in task, and they dealt with the industry in comments received in February 2003, in March 2003, and in April 2003.

Mr. SHAYS. Well, you confirmed this——

Mr. WELLS. They recommended to the NRC management that four of those categories I just talked about were lowered. Four of the five were lowered.

Mr. SHAYS. Right. So——

Mr. WELLS. It's a timing issue for us in terms of when the information was considered, which is recommended.

Mr. SHAYS. Yes, and what would be good is for us, when we meet behind closed doors, to walk through those. You know, in any case, were they strengthened?

Mr. WELLS. No, sir.

Mr. SHAYS. How did the NRC resolve the question of whether the DBT represents a true reflection of the terrorist threat and not based on basically what was viewed as practical?

In other words, it may be the design basis threat would be so impractical as to put the plan out of operation. But if that is the case, it should be put out of operation. I mean, if, in fact, the design basis threat is realistic, but not practical, that tells us something. Do you get the gist of my question?

Mr. WELLS. Yes, sir.

Mr. SHAYS. Let me ask Mr. Merrifield, since you haven't participated, if you would respond to that question?

Mr. MERRIFIELD. Well, I think part of that question goes to the heart of the question you asked previously, and that is regarding the involvement of the industry.

Mr. SHAYS. Right.

Mr. MERRIFIELD. The fact of the matter is we have a system in which we place the responsibility for defending the plants on the utilities themselves. So for the Commission to come up with a DBT in a vacuum without having an understanding of the impact operationally at the plants and what those costs would be would not be appropriate for us as a regulator to regulate in that way.

So I think it was important for us to have some sense of what the practicality of that may be and the associated cost.

Mr. SHAYS. You know, I think that is a very helpful and a very honest answer. But if you think about it, you could argue both sides of the equation. If, in fact, the design basis threat is realistic, but it is so onerous to the operation of the plant, it is still realistic.

Mr. MERRIFIELD. Well——

Mr. SHAYS. Let me just finish. So if it is realistic, that is the threat. And the threat really isn't an issue of whether or not it is practical. I mean, you may conclude that a particular plant needs to be shut down because the design basis threat is realistic—I am being redundant—but you can't defend it.

Mr. MERRIFIELD. I think there's a variety of elements that go into the decision that's made by the Commission. The first thing is taking the information that we derive from our own staff and from the intelligence community in attempting to derive what that threat is.

One of the things I think that we reflect on as Commissioners is the fact much of that information is subjective in nature. It involves judgment calls by the intelligence community regarding what they believe are the capabilities of the adversaries we face, and that salts its way throughout the early part of that process.

Layer on top of that is the interface between ourselves and our licensees and the responsibility that we place on them. We have, in the context of our regulatory authorities, the notion that there is an enemy of the State, some capability beyond which is really not the responsibility of our licensees, but in a free society is placed on local, State, and Federal Governments.

What we've tried to do as a Commission in a post September 11th environment is to enhance what we're doing with local, State, and Federal Government to make sure that the responsibility for defending the plant is seamless. Some responsibilities under the context of the DBT, which were imposed on our licensees, but coordinating under the auspices of DHS with our counterparts in local, State, and Federal Government to ensure that where the DBT ends off, there are capabilities out there to respond to those elements outside of the DBT.

Mr. SHAYS. Yes, sir?

Mr. MCGAFFIGAN. Mr. Chairman, let me just deal with the one that's the elephant on the table, the aircraft threat. Let's just take that threat. That was the September 11th threat.

Mr. SHAYS. Right.

Mr. MCGAFFIGAN. Dick Meserve, our former chairman, was testifying as early as 2002 that we did not think that threat belonged in a DBT because the weaponry with which you could defend yourself, either fighter planes armed with air-to-air missiles or surface-to-air missiles, is not appropriate for a private sector regulated guard force to have.

We didn't stop there. We then, I think, are unique in Government today in the relationship we have with NORAD and NORTHCOM, as they have upgraded their capabilities, we have imminent threat procedures at these plants. NORAD has high confidence they can detect the aircraft that are in duress nowadays diverting from a flight path.

If they can't get an F–16 there, they're on the phone with our licensees, and our licensees are prepared to put that plant in the safest configuration possible, which, among other things. If it's truly imminent, they will scram the reactor so the reactor is shutting down. There is no further nuclear energy being produced.

And they'll do various other things. Disperse personnel. All that sort of thing. The plants are inherently hard, compared to chemical

plants or anything else in our society. So we think that we have gone for. As Commissioner Merrifield said, in dealing with the enemy of the state, we don't stop there.

We work with the appropriate agencies of government. We have unique relations. The chairman was just at NORTHCOM and NORAD a few weeks ago with the senior staff to tighten that relationship. So that's what we do.

The original enemy of the state notion came when we were licensing—obviously, a previous Commission in the late 1960's—the Turkey Point reactor, which is less than 100 miles from Cuba, Chairman Diaz's home country, and with whom I'm sure he'd want me to add he strongly disagrees with Mr. Castro. [Laughter.]

Mr. SHAYS. What he would like you to say is he is a citizen of these United States, and proudly so, and grew up in Cuba.

Mr. MCGAFFIGAN. Right. The fact is that to deal with licensing Turkey Point, we had to assume the U.S. Air Force would intercept MiGs coming from Cuba.

Mr. SHAYS. Let me just say I understand, you know, that we have kind of slipped into the enemy of the United States issue, and that is a question of whether you incorporate in your design basis threat the responsibility to include that. And that is another issue.

The issue that we are not going to resolve, but the issue that, obviously, we are going to be wrestling with, as you do, is how much does practicality trump the design basis threat? That is the bottom-line issue.

Mr. Wells, do you get a sense of what I am asking here?

Mr. WELLS. I understand the sense of your question. It's an appropriate question. The GAO didn't make a value judgment about that.

Mr. DIAZ. Sir, can I——

Mr. SHAYS. And let me just say, before you respond, that we have been joined first by Mr. Platts, and appreciate him, from Pennsylvania and also our ranking member.

And I am going to make sure that I just take care of what is a technical responsibility of this Chair, and that is ask unanimous consent that all members of the subcommittee be permitted to place an opening statement in the record, and the record remain open for 3 days for that purpose. And without objection, so ordered.

I ask further unanimous consent that all witnesses be permitted to include their written statement in the record. Without objection, so ordered.

And to note for the record that we do have a quorum. We are legal. OK.

Yes, sir?

Mr. DIAZ. Let me go back to the question of, you know, how do you know that you have the right DBT, which I think is what you are asking.

Mr. SHAYS. Right. Right.

Mr. DIAZ. You know, I might have to beat our drums or toot our horns in here, but I want to assure you that since September 11th, these Commissioners and the entire Commission was so engaged on the issue of security that each one of us was continuously aware of what the intelligence that was coming, how it was being treated, how it was being handled.

Each one of us went and engaged other agencies. The process that we went through was very, very thorough and very comprehensive. We do take into account not only the intelligence threat, but what experts were telling. I personally went to the Department of Defense, sat down with the experts, looked at the information.

We made informed decisions. Those decisions that were made we made collegially. We interact. We bounce things off each other. This was a period of months in which we looked at everything that the U.S. Government had available, and I must say, sir, that we are very thankful that since September 11th, we got much better information. We got it quicker. We have tremendous amount of cooperation from other agencies.

We were able to receive information and make decisions that we believe were directed to protecting the public health and safety of Americans.

Mr. SHAYS. Before going to Mr. Kucinich in just 1 second, what I am interesting in knowing is—I mean, the bottom line is the staff made a recommendation. Obviously, staff is not always right. I am tempted to say more, but——

Mr. MERRIFIELD. They serve us all, Mr. Chairman.

Mr. SHAYS. Yes, they do. But the bottom line is they came out with a certain recommendation, and in four instances, I think you testified, Mr. Wells, they were softened. Four or five?

Mr. WELLS. Four of the five.

Mr. SHAYS. Yes. And so, were you told, "This was our recommendation, and now this is our recommendation based on input?" So you saw both. And did you question why they had been changed?

Mr. DIAZ. We saw the draft, and we saw the final recommendation. We went in closed doors with the staff and asked, you know, what is your best recommendations? What are the issues——

Mr. SHAYS. Did you ask them why they recommended it be reduced?

Mr. DIAZ. I don't remember that I asked them why. I questioned the changes.

Mr. SHAYS. OK. Well, we will ask you why when we are behind closed doors.

Mr. DIAZ. OK.

Mr. SHAYS. Just for the record.

Mr. Kucinich.

Mr. KUCINICH. Thank you very much, Mr. Chairman, and members of the subcommittee, to our witnesses.

Mr. Wells, in your summary of what GAO found, "GAO found that the process used to obtain stakeholder feedback created the appearance that changes were made based on what the industry considered reasonable and feasible to defend against rather than on what an assessment of the terrorist threat called for."

Is this conclusion based on what you would say would be the culture of the NRC itself in terms of its over-responsiveness to the cues which industry sends out about what it wants?

Mr. WELLS. Mr. Kucinich, we made that conclusion based on the process that we observed that was used in 2003 to develop that DBT. It was a timing issue in that DBT.

I would say that the NRC has responded to us that was a process that they don't normally use. That it was used to expedite the development of that particular DBT and that they believe they fixed our recommendation by saying that in the future they will not use that sequential process, but will revert back to an individual process step.

Mr. KUCINICH. So is it your opinion then that the industry is not calling the shots with respect to design basis threat?

Mr. WELLS. We have no evidence of that. What we say in our conclusion is because of the circumstances of when the comments were received and the staff that was used to receive those comments, it certainly could create the appearance that lest they could defend otherwise that they were influenced by the industry.

It's an appearance issue, a conflict of interest concern on our part.

Mr. KUCINICH. Right. Now, Mr. McGaffigan gave the subcommittee reasons why the private sector should not have to guard against air attacks on nuclear plants. My question is Mr. Wells—are there any security enhancements which could be made at sites to better protect against air attacks?

Mr. WELLS. Mr. Kucinich, in an open forum, we are aware of studies that have been done in a classified arena. But to discuss those details would be beyond the scope of this hearing.

Mr. KUCINICH. Mr. Diaz, is the Nuclear Regulatory Commission in contact with the industry with respect to fortifying reactors against potential air attacks?

Mr. DIAZ. The answer is not only are we in contact, sir. But on February 25, 2002, we ordered the industry to take measures to mitigate the consequences of large fires and explosions, including those that could be caused by aircraft attacks.

The industry was given requirements, timelines. Some of those, because they were made very quickly, had to be refined. But the answer is, yes, the industry has been ordered and is prepared to take those actions necessary to protect the American people from the consequences of aircraft attacks.

Mr. KUCINICH. Are you telling the committee that the NRC design basis threat includes aircraft attacks?

Mr. DIAZ. No, sir. I am not saying that.

Mr. KUCINICH. OK.

Mr. DIAZ. I am saying that we issued a specific order on February 25, 2002, that ordered the industry to be prepared, OK, to deal with the consequences.

Mr. KUCINICH. Mr. Chairman, considering that we know that the September 11th hijackers had initially targeted nuclear plants, why doesn't the NRC design basis threat include aircraft attack?

Mr. MERRIFIELD. Can I try that——

Mr. KUCINICH. Before you answer that, would it be OK if Mr. Diaz answered?

Mr. DIAZ. Sure. You know, fundamentally, this is an issue the Commission put a significant amount of thought. It was a serious issue.

You know, we have responsibility for both safety and security. We believe that we could deal with the potential consequences of

an aircraft attack in the safety arena, that we could actually require and did require our licensees to deal with the consequences.

We do not believe at the time, nor do I believe now, that we should make licensees responsible for defending, you know, with aircraft and anti-aircraft or any other measures against, you know, the anti-aircraft, against the aircraft threat.

Mr. KUCINICH. Well, now did Mr. McGaffigan want to add to that?

Mr. MCGAFFIGAN. Just, sir, the design basis threat is a legal term in NRC regulatory space. It's the threat against which the licensee has to be able to defend, as opposed to the enemy of the state concept that Chairman Shays started to get into, which is the responsibility of the Federal Government. And that concept has been in our regulatory practice for almost four decades.

The weaponry required for a licensee to defend against an aircraft attack—surface-to-air missiles and fighter planes with air-to-air missiles—that sort of weaponry is entirely inappropriate for a private sector regulated force to have.

Mr. KUCINICH. I don't know that anyone here is suggesting that the licensees do that. But there was a suggestion earlier with respect to fortification of the reactors.

Mr. MCGAFFIGAN. But, sir, we have, as Chairman Diaz just outlined, as a result of the February 27, 2002, order—February 25, 2002, order asked licensees to figure out what they can do to cope with an accident should it occur, should such an attack occur, with their safety systems, what enhancements can they do with their safety systems.

As I said in response to Chairman Shays earlier, we can put the plant, we think with the help of NORAD and NORTHCOM, in the safest possible configuration that we can place it with a little bit of warning, and we have procedures in place, tested procedures in place to do precisely that.

So we think that the combination of our imminent threat procedures, the inherent hardness of the facility, the additional thought that licensees have given to this matter since February 25, 2002, adds up to a very robust capability to protect the public health and safety.

Mr. KUCINICH. Have all the licensees complied with your communications?

Mr. MCGAFFIGAN. Yes, sir.

Mr. KUCINICH. If they have all complied, you know, I understand that nuclear plant owners applying for license extensions are required to submit a severe accident mitigation analysis as part of their applications for renewal of their licenses.

Why doesn't the NRC require a design basis threat analysis of an aircraft attack in the severe accident mitigation analysis?

Mr. DIAZ. The design basis threat rulemaking will take into consideration, according to what the comments and what the process finally ends up, the potential for an aircraft attack, that we believe that the rulemaking is the right process to be able to get the right information on the issue, proceed with, you know, the deliberations that need to take place.

So it will be part of the new consideration of the DBT. And if, at the time, that is a pathway, then we will take it very seriously and consider it.

It might very well be that we, at the time, the U.S. Government will have enough additional protection for aircraft that added to the defenses that exist at the plant for the safety systems, you know, we might consider that might not be adequate. I cannot prejudge what the decision will be.

Mr. KUCINICH. Yes, I want to go back to Mr. Wells. According to the GAO, the NRC, under pressure by the nuclear industry, overruled staff recommendations in the draft design basis threat that required a full range of weapons that could be expected to be used in an attack on a nuclear facility.

My question to you is did the NRC staff recommendations in the draft design basis threat also include a large aircraft as one of the weapons that could be used in such an attack, and did the NRC overrule such a recommendation?

Mr. WELLS. The staff did not include an airborne——

Mr. KUCINICH. I am sorry?

Mr. WELLS. The staff did not include a recommendation for airborne protection in the draft DBT.

Mr. KUCINICH. So the staff never mentioned on staff recommendations. There is no draft staff recommendation for aircraft?

Mr. WELLS. To include airborne, there were not.

Mr. KUCINICH. None? And so, therefore, the NRC didn't overrule——

Mr. WELLS. That's correct.

Mr. KUCINICH [continuing]. Because you said such a recommendation was never made?

Mr. WELLS. That's correct. For airborne. For other weapons and equipment, yes. But not for airborne. It was never included originally.

Mr. KUCINICH. OK. One final comment here, and that is that the concerns which some of us have is that the industry is basically leading this dance, and the industry may not want to spend the kind of money that would be necessary to fully protect these nuclear reactors.

And that it is up to the NRC to tell the industry what it ought to do. It is not up to the industry to tell the NRC what it is willing to do. There is a difference of opinion.

Thank you, Mr. Chairman.

[The prepared statement of Hon. Dennis J. Kucinich follows:]

Statement of Rep. Dennis J. Kucinich
Ranking Minority Member
House Subcommittee on National Security, Emerging Threats and International Relations
Committee on Government Reform
U.S. House of Representatives

Hearing on "Nuclear Security: Has the NRC Strengthened Facility Standards Since 9/11?"

April 4, 2006

Good afternoon, Mr. Chairman, and welcome to all of the witnesses here today.

This Subcommittee has held multiple hearings on both the Department of Energy's and Nuclear Regulatory Commission's (NRC) implementation of the Design Basis Threat (DBT) since it was revised in April 2003. Based on the most recent intelligence analysis, the DBT predicts the need for commercial plants to defend against an even larger, more sophisticated, and lethal terrorist attack force.

But while the GAO report released today generally praises NRC and industry efforts to upgrade security at plants, one finding should raise an eyebrow. GAO found that NRC commissioners sought industry feedback regarding types of weapons that could be used for an attack at a plant, and then rejected their own staff recommendations to require plants defend

against these weapons after the nuclear industry stated that it was too expensive. Moreover, the commissioners did not justify their decision to overrule their own analysts by providing the criteria used to arrive at their decision. Frankly, this doesn't pass the smell test.

This constant catering to industry demands, collusion, and instinctive secrecy, should come as no surprise. It is exactly what Americans have come to expect from the nuclear industry. Just as it is erecting barricades at the plants, the industry is also putting up new barriers between the industry and the public. We need more information and greater openness from the NRC and industry, particularly when it comes to safety and security issues. Given its reactions to recent events, this basic lesson still has not been learned.

For example, the acid leak in the reactor vessel at the Davis-Besse nuclear plant in Ohio in 2002 was the most extensive corrosion ever found at a U.S. reactor, and had worsened over a four year period. Yet, cover-up by employees of the plant's owner, First Energy, along with the flawed risk estimate of the NRC, allowed the plant to continue operating. The focus of First Energy was on profits, not on safety, and it placed the people of Ohio in grave danger. Only this year has First Energy acknowledged its cover-up

and agreed to pay $28 million in fines in exchange for avoidance of criminal charges by the Department of Justice.

In April 2005, a National Academy of Sciences report concluded that a passenger plane flying at high speeds could cause fires and disperse large amounts of radiation if it deliberately crashed into a commercial nuclear plant. But rather than make security changes, the NRC fought to keep this report out of the hands of the public.

The NRC has also pulled safety information from its website, restricted access by public interest groups, and even tried to keep inspection and security guard performance information secret.

Last fall, an ABC News investigation found that security at 25 college campuses with nuclear research reactors was full of security holes. The investigation found unmanned guard booths, guards asleep on the job, unlocked buildings, and no metal detectors at any of the facilities. At Ohio State University, visitors were able to gain access to high-security areas with no background checks, and did not have their bags screened.

So while I believe these oversight hearings are productive, and have spurred some changes in the security at our nation's nuclear plants, the reality is that we have a long way to go.

That's why these questions must be posed and answered in an open and honest dialogue with industry. Billions of dollars may be being spent on physical security, but Congress needs to make sure we are getting the truth from the regulators, licensees, and utilities that the changes made are effective and long-lasting. The nuclear industry needs to come clean and admit the real problems which plague their industry, and which affect the American people.

I hope we will have such a frank dialogue today, and can do what's best to protect all Americans, not just the plant owners.

Thank you, and I yield back to the Chair.

Mr. SHAYS. I thank the ranking member very much.

Mr. MERRIFIELD. Mr. Chairman, may I respond to that?

Mr. SHAYS. Sure.

Mr. MERRIFIELD. May I respond to that briefly?

Mr. SHAYS. Sure.

Mr. MERRIFIELD. I would say I appreciate the comment made, Congressman Kucinich. I think we take our independence very seriously. We are willing to issue orders for security. We have issued very significant, very costly orders for security in a post September 11th environment.

We certainly, as we listen to stakeholders, whether it's Congress, whether it's the American people as a whole, or whether it is the utilities that we regulate, we listen to the views of a myriad of people who have concerns about these issues.

But at the end, the members of the Commission, including the three of us who are here, were sworn to uphold and defend the interests of this country. And so, we take that mission very seriously in making an independent judgment as to what we feel is appropriate, irrespective of whether the industry likes it or not.

Mr. KUCINICH. Mr. Chairman, if I may, in response?

We know the NRC has pulled safety information from its Web site, restricted access by public interest groups, even tried to keep inspection and security guard performance information secret. Sir, with all due respect, I have my own understanding of the NRC with respect to the conduct of the NRC at Davis-Besse in Ohio.

So I want to take what you are saying in the spirit that you are going to do the best job you can. That is how I want to take it. But I also know that the NRC is under different types of pressures that some agencies come under when there is powerful interest groups at work.

So thank you for the job you are doing.

Mr. SHAYS. Mr. Platts. Thank you, Mr. Platts, for your patience.

Mr. PLATTS. Thank you, Mr. Chairman.

I apologize. I need to run to a 3 o'clock meeting, but I do appreciate the chance to get a couple of questions in.

Mr. SHAYS. You take your time.

Mr. PLATTS. Thank you for your continuing oversight of this issue.

I want to just make sure my understanding, Mr. Wells, in your testimony here today and your written statement, you have talked about that appearance of a conflict and that the industry's input that it was really what was reasonable and feasible to defend against, as opposed to an assessment that was based on the realistic terrorist threat. And that there was an appearance of this.

I don't know if you are able to answer in this session or when we are in closed session, but besides the appearance, is there a belief by GAO that is the fact. That it was a decision based on the reasonable and feasible in the industry's perspective, as opposed to the good faith terrorist assessment?

Mr. WELLS. We have no evidence to support undue influence by the industry. It clearly was an appearance issue to us that we believe could be fixed if the threat assessment staff were just removed from this process.

What we do know factually is what they recommended going in, after getting industry and other's comments, was lowered significantly in terms of their recommendation to the Commission for approval. That's what we know.

Mr. PLATTS. In being lowered, is it then your opinion that the lowered standard is not in line with the realistic threat?

Mr. WELLS. We did not make an evaluation judgment or were we asked to decide whether these decisions were correct. So we just reported on the process that occurred.

Mr. PLATTS. OK. Thank you.

On the specific issue of the inspections and the force-on-force exercises, my understanding from the testimony is less than half, 27 of the 65 have had force-on-force exercises.

Mr. WELLS. Thirty-one, 30-some percent. That's correct.

Mr. PLATTS. OK. This would be a question really to the Commission members or to you, Mr. Wells. Is there a timeframe for when all 38 remaining will also have had those exercises?

Mr. DIAZ. Yes, sir. They all have to have an exercise within a period of 3 years. In the next approximately 15 months, they would all—will have conducted force—a new, complete force-on-force exercise. You miss the fact that we have been having other not as complete force-on-force exercises.

Mr. PLATTS. Right.

Mr. MCGAFFIGAN. Excuse me, sir. Could I also add——

Mr. PLATTS. Sure.

Mr. MCGAFFIGAN [continuing]. That one item of our training requirements for the power reactors is that every shift of security personnel gets trained annually, which de facto becomes they do force-on-force exercises at least quarterly. They have five shifts. They get them done, and there are very impressive capabilities they have for their own force-on-force exercises to get ready for our scored force-on-force exercise.

I was at Quad Cities last week. Exelon—you'll have Mr. Crane later—has chosen to buy its own MILES gear. So they use this equipment that comes from the military that makes the exercises much more realistic, even in their own training exercise. Not waiting for us to show up.

So that's an example, I think Mr. Wells mentioned earlier, where licensees have gone beyond NRC regulatory requirements. So our exercises, our scored exercises occur once every 3 years, just as Congress asked us to do in the Energy Policy Act. But our training requirements require them to do force-on-force exercises more than once a quarter.

Mr. MERRIFIELD. Well, and just very briefly?

Mr. PLATTS. Sure.

Mr. MERRIFIELD. In addition, because we have resident inspectors at the site, they do have the opportunity to also witness those additional exercises. We don't evaluate those formally or grade them on them, but obviously we take what we do from observing those.

Mr. PLATTS. The requirement that at least once in the 3 years, the force-on-force, is the reason that there are still 38 that have not had that just a manpower issue, being able to plan and execute those 38?

Because given the environment we are in, the fact that we are 4 1/2 years after September 11th and still another 15 months perhaps until we get all of them done, it seems like we would want to be prioritizing that.

Mr. MERRIFIELD. I think, just to clarify one thing, we have been conducting force-on-force evaluations at the plants pre September 11th. We've been doing it since probably the mid 1980's or before—early 1990's?

Mr. DIAZ. Early 1990's.

Mr. MERRIFIELD. What we've done, however, is we have reduced the periodicity of those. We used to make sure we had 1 every 7 years. Now we're to 1 every 3 years. We're increasing the rate of this.

Mr. PLATTS. Right.

Mr. MERRIFIELD. But I just didn't want to give you the impression——

Mr. PLATTS. Also, the assumptions that you are basing those force-on-force certainly have changed.

Mr. MERRIFIELD. Agreed. That's correct.

Mr. PLATTS. Because of what happened on September 11th, and not just September 11th, but throughout the 1990's with the different major terrorist attacks against our Nation.

Mr. MERRIFIELD. That's absolutely right. What is different about the new ones that we're taking a look at is, No. 1, they're better exercises. We use a MILES gear, as Commissioner McGaffigan has mentioned. We test them harder. We test them with more elements. So it's a better exercise now.

But I just didn't want to leave the impression in the record that we somehow invented force-on-force 3 years ago because we've been doing this for many, many years.

Mr. PLATTS. Right. Mr. Chairman.

Mr. DIAZ. And there is one key fact is that——

Mr. SHAYS. Excuse me. You may be the chairman, but you still have to use the mic. [Laughter.]

Mr. DIAZ. Thank you, Mr. Chairman.

One key fact is that the way these exercises have been distributed among the industry is that 31 out of 32 licensees have experienced one exercise or another. So they all have been exposed to it, OK?

So that means that in their security culture, they have been exposed to it. They have seen it. They know what it is. They know what the requirements are. They actually are then capable of taking these experiences from one plant to the other, and I think that is a very favorable fact.

Mr. PLATTS. Let me get one other quick question, I apologize in having to run. That regarding the frequency of the inspections. Mr. Wells, in your testimony, you talk about that they have improved their force-on-force, for example, by conducting inspections more frequently at each site.

So does that mean some sites have had more than one force-on-force exercise while others are still waiting?

Mr. WELLS. In the past, these exercises were conducted in a different form but were done once every 8 years. They've escalated that to once every 3 years. I do want to point out that's still an

aggressive schedule. These things are big deals. They're very expensive to conduct. And it's going to be a challenge for them to complete all these in time.

Mr. PLATTS. So I want to make sure I am not misinterpreting. There has been no facilities that have had a second force-on-force in the 3 years before others have had their first?

Mr. WELLS. With the exception, if they perform a force-on-force, and the licensee performs poorly or there is unanswered questions about their ability to protect, they will schedule a second, repeat exercise.

Mr. PLATTS. OK.

Mr. WELLS. They'll keep going back to that same plant until they get it right.

Mr. PLATTS. OK.

Mr. DIAZ. We have done that, Congressman. We had one plant that did not meet standards, and we scheduled immediately another force-on-force within 3 months, went back. And then that time, they were ready.

Mr. PLATTS. Glad to hear that, and—yes?

Mr. MERRIFIELD. Yes, I just want to add one thing I think goes to your previous question. One additional enhancement that hasn't gotten on the record today is the quality of the adversary force.

Prior to the changes that we made, they used to use personnel at the plant as the adversary force or from other individuals who work for the utility. Today, the adversary force is made up of individuals typically who have special forces background, delta force background.

These are very highly capable, very motivated individuals who truly want to test what these plants are doing, and we believe that's a real enhancement to the quality of the overall exercises.

Mr. PLATTS. Well, maybe that actually raises; so they are employees of NRC?

Mr. MERRIFIELD. No, they are not. They are actually——

Mr. PLATTS. Or they are still contracted?

Mr. MERRIFIELD. They are contract employees.

Mr. PLATTS. But not from the industry participant?

Mr. MERRIFIELD. No, they are not employees of the industry, not from the utility.

Mr. MCGAFFIGAN. They are from industry. I mean, we can get into this. NEI contracts with these folks. Wackenhut provides the people. They take them from across the industry. So guards volunteer for this duty. We have a substantial force of people to draw from in order to staff each exercise, as Mr. Wells talks about.

We make sure that there's no undue influence. There's a bunch of conflict of interest requirements that we have imposed that we believe adequately protect against a conflict of interest there.

But the fact is that these people are much better than anything we had before, and we're managing any conflict of interest issues we think very adequately. There's no "Keystone cop" routine when they are at a site that Wackenhut happens to have the security force at.

Mr. PLATTS. Knowing I am going to be even later now for my meeting that you keep raising additional thoughts. Is there any consideration to NRC that volunteer actually being engaged to be

NRC's own team so you avoid even the possible appearance of that conflict, that they are NRC employees who are fully dedicated to this responsibility?

Because given how often you are doing them and they are going to continue to do them, it would seem natural that you would have your own in-house team.

Mr. DIAZ. No, sir. We are not giving serious consideration to that because we actually run this adversary forces in many ways. We provide the scenarios. We provide the qualifications. We provide the requirements. We do the scheduling.

We believe that it's critical for these facilities to maintain a distinct separation between what would be an external component to their plants and the safety of the plant. We want safety and security to be integrated in the plant so that they could work together synergistically and actually do a better job together than they can do if they are independent of each other.

Mr. PLATTS. But it sounds like that the team actually carries out what NRC devises as a plan of attack that they are going to go through in their exercise?

Mr. DIAZ. That is correct.

Mr. PLATTS. OK. I apologize that I need to run out. Final thought?

Mr. MCGAFFIGAN. I'm the Democrat on the Commission, sir, and it's a resource issue partly. You can ask NEI later what they pay annually, but it's millions of dollars, I think close to $10 million a year to keep this force in shape. And it didn't strike us—we thought we could get the same benefit without adding those employees.

Furthermore, we think there is a benefit. These people are going to rotate off of the adversary force back to their licensee, and they can bring the knowledge that they gained as these folks are the best people that attack the nuclear plants on the face of the Earth. They'll bring that knowledge back to their site——

Mr. SHAYS. I am going to cutoff this discussion only because I think you have made the point well.

I am going to have to speak before the Rules Committee sometime soon, and we are not dismissing you yet because I want to just get to one other area, and that is criteria.

Mr. PLATTS. Mr. Chairman, I appreciate your patience with my exchange——

Mr. SHAYS. See, the problem was, you were to come back and relieve me. And now you are going to be late there. So I am getting screwed on both ends here. [Laughter.]

But the questions were great.

Mr. PLATTS. All the more my apologies, Mr. Chairman.

And my thanks to the Commissioners, Mr. Wells, to all of your efforts and testimony here today. Thank you.

Mr. SHAYS. Thank you. They were good questions. Thank you for coming.

I am going to have the professional staff ask questions. I would like one Commissioner to answer, not three, on this so I can get through, unless the answer does need additional magnification. And I have focused on criteria.

Mr. HALLORAN. There is the lingering dispute between the GAO and the Commission about the question of criteria for decision-making about the DBT standards. That your testimony makes statements to the effect that detailed and restrictive criteria could be detrimental to the Government and could overly limit your discretion.

But in one sense, that is the easy case. That is not necessarily what was recommended. Let me ask first, what kind of criteria were you recommending; to the extent you can talk about that out loud—and are there precedents for it elsewhere in other regulatory settings that you have seen?

Mr. WELLS. We did not recommend or specify a specific criteria. We assumed that the NRC would develop their own criteria. So their concern about anything being unduly prescriptive would be up to them to decide what type of guidelines and in terms of what factors should be considered, the types of weight that may be given to those factors.

We have found throughout government, where decisionmakers have been asked to consider risk management and make informed decisions based on risk considerations, that there's been great value in guidelines that are available to the decisionmakers that lay out all the various factors and provide some weight to them to assist them in having a very defensible transparent reasons why the decisions were made one way or the other.

We found that rigor improved the consistency of how decisions were made, coupled with the fact that they were semi-annually reviewing these DBT recommendations. So the process is ongoing, happens frequently, and we just found value in having the written guidance that we believe NRC should develop themselves.

Mr. DIAZ. I respectfully disagree with that conclusion, and the reason is that the Commission has very straight means in which to make decisions. We receive information. We interact.

Anything that will come and put a rule, what it would do is we will start paying more attention to the staff, paying more attention to what the criteria are than what the circumstances are, what additional information is. I think this is a deliberative body that meets frequently——

Mr. SHAYS. Let me just interrupt a second and get through this. One of the questions I might have asked, is it possible to have criteria? And then logically it is.

It seems to me you are almost interviewing someone for a job without having some basic standards and requirements you go through. You seem to interpret the criteria maybe because you follow so many regulations. We are not saying that it limits you that you only have the criteria that you establish. You might add or subtract to the criteria as you work this process through.

But when you interview someone for a job, you know what you are looking for. You have certain things on your list. You know what the job entails. Then you look for that match.

And you just don't do it subjectively and sit down and say, "Oh, he seems like nice guy." And all of us say, "Oh, yes, let us hire him." And that is kind of the feeling I get.

Mr. MCGAFFIGAN. Mr. Chairman, just so you know that we're not a phalanx here. I have advocated for the GAO position internally.

I believe we tried in 2003 to come up with criteria briefly. We didn't agree. We don't agree on the criteria.

We tried more recently. In the last semi-annual threat assessment, the Commission response to the last semi-annual threat assessment, I again proposed criteria, and we didn't reach agreement. I personally believe we should have criteria. But our two attempts at arriving at criteria failed.

Mr. SHAYS. Let me just see, I would think you would have criteria and then add to it or subtract to it. But you would have some basic criteria that you would follow. It seemed very logical to me. I would, if I had been on the Commission, would have supported you.

No, I mean, I appreciate you pointing that out. We don't all agree in Congress. You don't all agree on the Commission. If you all came with one voice here, I would be pretty unhappy about it.

I at least would like to know that you are debating that. That is a healthy thing. And I guess what I would say to you is I hope you keep at it until you feel you can find some agreement.

It is not locked in stone, you know, chipped in stone. I would think you would constantly re-evaluate the criteria.

Do you mind, gentlemen, if we go on? I usually say is there anything we should have asked that you wished we had, but I don't want to know that. [Laughter.]

Yes, I already spilled water on you. That is good enough.

Mr. MERRIFIELD. Mr. Chairman, I know you want to get through this question, but I would like to just fill something in.

Mr. SHAYS. Sure.

Mr. MERRIFIELD. Because we confronted this when we had our meeting with the GAO staff, and they asked us how we went through our decisions. And I think we can go into more detail on this when we have a closed session.

Part of this is ultimately like the decisions that you make as a Member of Congress, judgment calls. It's based on the myriad of information you have available to you.

When we met with the GAO staff, they said, well, in coming up with the DBT, can you give us the list of documents you used to make your decision? And part of my answer was I've been a Commissioner for 7 1/2 years. I've had access to thousands of pages of highly classified documents.

I made visits to all 103 nuclear power plants in the United States and, indeed, half the nuclear power plants in the world. I visited with colleagues in any number of agencies. I met with well over 100 Members of Congress since I've been a Commissioner. Those are the kind of things that you use to make an informed decision.

Now my disagreement in terms of Commissioner McGaffigan, in terms of having a set of criteria is I think the Commissioners, each of us as independent Commissioners, has to have some of those criteria in our own minds, as you do when you are making a decision on immigration reform or other things.

Commissioner McGaffigan will tell you, he and I have some very vigorous discussions about these issues, which I——

Mr. SHAYS. You know what I am sensing, though? You are a Commission that has to dot your "i's" and cross your "t's." So I

think you tend to think of criteria as almost being a restriction. I would think it would be a basis if in the end you decide to override a criteria, then there would be an explanation that you would be able to give.

But my sense is you all should keep working at that because I have a feeling that if someone analyzing a business structure would say, you know, this is very doable.

Yes, on a bill, I don't follow the same criteria for every bill. I use what I call my "community meeting test." If I can't explain it at a community meeting, I better not do it, you know?

But it is a criteria, you know? And so, if someone says, "Why don't you go to the Paris air show," and I talk to my staff about it. They say, "Hey, boss, you are not on the aviation committee. You are not even on transportation. I don't think it meets your test."

I mean, there are certain things that I would think you would have, and I would think you would be able to even write them down collectively.

Mr. MERRIFIELD. Well, Mr. Chairman, I certainly agree with you. That internal decisionmaking is the same way you do, we all have decision criteria that we use. I mean, I'm very proud of the fact that when my staff tries to gauge where I am on an issue, they're going to be able to understand with about a 98 percent accuracy what I intend to do because I use those very same kind of criteria.

I think there is a concern about the Commission as a whole being locked into a single set of criteria, when each one of the five of us brings our own value judgments.

Mr. SHAYS. OK. I am going to have to get the last word, which is the privilege of the chairman.

I hope that you take seriously the recommendation or concern of the GAO and that you continue to debate this and that you continue to evaluate whether you could come up with a criteria that would make sense. It then gives us the benchmark to which to evaluate as well.

I think it would provide for a meaningful discussion. So I realize there is disagreement here, and that is the way we will leave it, but at least you know where we are coming from.

Thank you. You have been a very responsive panel, and I thank you very much for that.

And thank you all.

We are going to get onto the next one, and if you would stay standing, I will swear you in.

We have the Honorable Richard Blumenthal, the attorney general of the State of Connecticut and, for the public record, a close friend. We have Danielle Brian, executive director, Project on Government Oversight. We have Mr. Marvin Fertel, vice president and chief nuclear officer, Nuclear Energy Institute. And we have Mr. Chris Crane, president and chief nuclear officer, Exelon Generation Co.

Mr. Chris Crane? Yes. Oh, I am sorry if I said it incorrectly. It is Mr. Chris Crane. Stay standing.

I don't always get to swear in the attorney general of the State of Connecticut. So this is a real privilege.

[Witnesses sworn.]

Mr. SHAYS. Note for the record, all four have responded in the affirmative.

And I just want to note for the record, we have Mr. Duncan from Tennessee, who has been a wonderful member of this subcommittee. And we might be able to persuade him to chair this subcommittee if I have to go to the Rules Committee, but we will see how that works out.

The Honorable Richard Blumenthal. Dick, it is wonderful to have you here, and thank you for your outstanding service, and thank you for serving in your capacity as attorney general. You do a terrific job.

STATEMENTS OF RICHARD BLUMENTHAL, ATTORNEY GENERAL, STATE OF CONNECTICUT; DANIELLE BRIAN, EXECUTIVE DIRECTOR, PROJECT ON GOVERNMENT OVERSIGHT; MARVIN FERTEL, VICE PRESIDENT AND CHIEF NUCLEAR OFFICER, NUCLEAR ENERGY INSTITUTE; AND CHRISTOPHER CRANE, PRESIDENT AND CHIEF NUCLEAR OFFICER, EXELON GENERATION CO., LLC

STATEMENT OF RICHARD BLUMENTHAL

Mr. BLUMENTHAL. Thank you very much, Congressman Shays, Mr. Chairman, members of the subcommittee.

First of all, let me thank the chairman, Congressman Shays, for his real courage and conviction on this issue, his continuing oversight, and his recognition about the importance of openness, increasing the amount of information available to the public on this issue. Because what's at stake here, as much as anything, is the credibility of this process.

And so, I want to first thank him for his enormous contribution on that score and just say that——

Mr. SHAYS. I would just like to point out to the rest of the panelists, you do not need to do this. This is a Connecticut thing. It has been all taken care of. So we will get right to the point there.

Mr. BLUMENTHAL. And he's my Congressman.

I also want to say that nothing I have to say here questions the good motives and dedication of the panel that preceded me or anyone else involved in the Nuclear Regulatory Commission. We do have differences, as the chairman pointed out. And on those differences, I think that I'm going to rely principally on my written testimony. But I think credibility will depend on having criteria.

Very clearly, there need to be criteria, particularly for the selection of weapons. The decision to drop, for example, two of the weapons that were recommended by the staff, as reported by the GAO, calls into question seriously and severely the credibility of the entire process, as do other apparent failings, such as the complete failure to involve potential air attack, particularly from the larger kinds of aircraft that could pose a threat at places like Indian Point, which is very much of concern to me, the Indian Point power plant being located so clearly and closely to the large part of Connecticut's population.

An air attack is not simply a speculative or imaginary kind of occurrence. It is a clear and present danger. The idea that there is a distinction between enemy of the state and design basis threat

that justifies excluding air attack seems completely unrealistic and unfounded.

I believe that the NRC must be required to give more reliance to the security experts, homeland security experts, people who are objective and independent of this process rather than nuclear power plant operators.

As the GAO report very pointedly observes, weapons were removed from the DBT after the nuclear operators were consulted and after they submitted their views on the feasibility and cost and said that, "Certain kinds of adversary characteristics would be prohibitively expensive."

I agree with the GAO that this situation created, "created the appearance that changes were made based on what the industry considered reasonable and feasible to defend against rather than an assessment of the terrorist threat."

Again, credibility is at stake here, and the public not only demands and needs, but also deserves credibility in this process, which would include prescriptive criteria, detailed criteria on what should be involved in this process.

I want to emphasize that there needs to be greater emphasis on the potential threats posed by spent nuclear fuel pools. The presence of such pools is a real factor in Indian Point and at Millstone. Some of them are housed in structures that are comparable to the kind of pools that we swim in rather than the ones we store nuclear fuel in.

The hardening of the domes encasing the plants may be deemed adequate, although I'm not necessarily conceding they are. But certainly the spent nuclear fuel deserves and needs greater protection.

And I want to emphasize also the importance of protection for whistleblowers. We are engaged right now in a specific case that involves a whistleblowing complaint and then a retaliation. I've asked, as recently as last week, the NRC to investigate in their annual assessment, I've asked them to investigate.

I think the NRC must provide protection for whistleblowers and investigate whenever whistleblowing kinds of allegations are made, and there are indeed indications of retaliation. Only yesterday I called on the NRC to immediately investigate the source and extent of radiation contamination at Indian Point.

Last week, the plant operators admitted that radiation levels in wells as close to 50 yards of the Hudson River were three times the allowable levels for drinking water. Environmental threats have to be the subject of NRC attention as well, and certainly Indian Point has posed them.

Let me just conclude, and I know that your time is short, Mr. Chairman, and I appreciate your staying this long. Conclude by saying that the kinds of attack that may be made in the view of many experts has been gravely underestimated. The potential for multiple terror cells or different kinds of weapons or larger scale attack all seem to have been underestimated in the design basis threat that has been in use so far.

So, I hope that this committee will begin to persuade the NRC and, if necessary, compel it to think outside the box, think of threats that have not been considered before, air attacks, air exclusion zones, the kinds of threats posed by traffic in Long Island

Sound—LNG tankers that may be part of energy projects—all need to be assessed and considered.

Thank you.

[The prepared statement of Mr. Blumenthal follows:]

RICHARD BLUMENTHAL
ATTORNEY GENERAL

Office of The Attorney General
State of Connecticut

TESTIMONY OF
ATTORNEY GENERAL RICHARD BLUMENTHAL
BEFORE THE SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND INTERNATIONAL RELATIONS
OF THE HOUSE COMMITTEE ON GOVERNMENT REFORM
APRIL 4, 2006

I appreciate the opportunity to speak on the critically important issue of nuclear safety, particularly regarding whether the Nuclear Regulatory Commission (NRC) has adequately strengthened safety standards for nuclear power plants since 9/11.

Connecticut's experience and a recent Government Accountability Office (GAO) study demonstrate the urgent need for renewed and reinvigorated NRC action to ensure the safety and security of our nation's nuclear power stations in this age of terrorism. Congressional action is critical because nearly 25% of our country's electricity is generated at 103 nuclear power stations -- many located near major population centers.

Congress should:

- Require NRC to give priority to national defense and homeland security experts in making the ultimate determination as to the type of possible attack on nuclear power plants -- and reduce the NRC's reliance on nuclear power plant operators in making such decisions.

- Demand that the Design Basis Threat (DBT) give greater emphasis to potential threats to spent fuel pools. The DBT currently focuses on the nuclear power plant itself. Spent fuel pools often contain significantly higher amounts of radioactive materials than the reactor.

- Carefully review the DBT to ensure adequate consideration of certain types of potential attack -- by planes larger than Boeing 707 airliners for example, and other threats -- and recommend effective measures to deter such strikes.

I have been deeply involved in safety and security issues at nuclear power plants because Connecticut is home to the Millstone Nuclear Power Plants and nearly one third of Connecticut's population lives within the 50 mile possible contamination zone of the Indian Point Nuclear Power Plant in Buchanan, New York. Radiation from an attack or accident could quickly create

a major public health crisis or catastrophe. In the event of an accident or attack, millions of people will need to be evacuated either from or through Connecticut on our three interstate highways. Losing a major generating facility at a time of peak demand could cause paralyzing regional blackouts creating turmoil and panic.

Forestalling attacks on these facilities must be an urgent priority.

Persistent reports of inadequacies in security planning at many nuclear facilities should compel Congress to require stronger action by the NRC. Despite clear calls to action, based on compelling evidence, the NRC has failed to address adequately security issues at Indian Point and whistleblower allegations at Millstone. The GAO report provides glaring accounts of NRC failure to adequately plan for terrorist attacks on our nuclear facilities.

Indian Point is a serious security and safety risk. The nuclear power plant operators have compiled an unacceptable records of abject, repeated, multi-year failure to effectively address vital safety and security issues. My office and New York-based Riverkeeper, Inc. have filed numerous administrative actions and court challenges to the demonstrably inadequate radiological emergency preparedness plan (REPP). There have been published reports of the potentially inadequate design of the reactor protection system and repeated failures of the facility's onsite electrical safety systems since 1999.

Yet, the NRC has consistently and repeatedly rebuffed requests -- from me as well as other public officials and citizen groups -- for NRC reviews and audits of the emergency preparedness systems at the Indian Point Nuclear Power Plant. This facility is only a few miles from the Connecticut border. Several New York and Connecticut senators and congressmen have submitted legislation -- which I support -- requiring a thorough, comprehensive NRC review.

Yesterday, I called on the NRC to immediately investigate the source and extent of radiation contamination at Indian Point. Last week, the plant operators admitted that radiation levels in wells as close as 50 yards from the Hudson River were three times the allowable levels for drinking water. The operators and regulators agree that the radioactive strontium-90 has found its way into the Hudson River. Strontium-90 is so dangerous to infants that its dissemination as part of the fallout from nuclear weapons testing led to the ban on above-ground weapons testing.

The NRC has also failed to address adequately allegations by a Connecticut whistleblower regarding the Millstone Power Plant. The whistleblower, a former employee at the Millstone Nuclear Power Plant, complained about failures of the plant's perimeter security system caused by false alarms. When these false alarms occur, the alarm system may be shut down entirely. Evidently, this problem has persisted for some time.

As troubling as this security deficiency, is the claimed retaliatory dismissal of this whistleblower employee. No facility can be safe if it punishes employees who speak out seeking to enhance safety. While the NRC has been silent, the Connecticut Department of Public Utility Control has reviewed the allegations and opened a public docket on the issues.

Congress can compel the NRC to be more effective in monitoring and scrutinizing safety systems. A culture and rule of safety, rather than intimidation, must be enforced at every nuclear power station.

I have some specific comments about the GAO report on the NRC's Design Basis Threat.

Design Basis Threat

The central core of design basis threat analysis is the proper assessment of various possible forms of attack on nuclear power plants. The NRC appropriately consulted with various defense and homeland security experts to develop this assessment. Inexplicably, the NRC weakened the list of potential forms of attack by allowing the operators of the nuclear power plants -- who have fiscal reasons to reduce the expenses involved in defending themselves from these possible attacks -- to edit and change the assessment. In particular, the NRC concluded that multiple terrorist cells are unlikely to attack one nuclear power plant. Yet, multiple attacks at one site are precisely what occurred on September 11, 2001.

The resulting assessment fails to fully reflect the defense and homeland security expert comments as to various possible forms of attack and, consequently, fails to adequately address the types of attack that were deleted or minimized.

Al Qaida has not hidden its intention to strike "decisive blows" against the United States Economic targets, particularly including energy supply infrastructure systems, have been attacked by Al Qaida in other countries, including Saudi Arabia and Iraq. An Al Qaida spokesman has stated that while they initially chose not to attack nuclear power stations, circumstances have changed and such facilities are considered legitimate targets. Published news reports have indicated -- for example -- that plans for the Indian Point power station have been found in a cave in Afghanistan purportedly used by Al Qaida.

We know all too well that Al Qaida has demonstrated an intention and capacity to stage medium to large scale terrorist attacks on U.S. soil. Terrorist use of multiple attackers -- 19 in 9/11 for example -- means that the NRC must mandate that nuclear power stations be prepared to defend successfully against a substantial organized force. There is no reason to believe that NRC's current, supposedly enhanced DBT assumes threats from more than a handful of attackers. To the contrary, the DBT is predicated on the clearly dubious assumption that an attacking force will be much smaller. This assumption is certainly disputable and compromises the entire security plan.

Similarly, the GAO report noted that the NRC removed from the design basis threat two types of weapons that NRC staff recommended for inclusion. This step followed objections from the nuclear power plant operators.

The attacks on the Khobar Towers in Saudi Arabia and the U.S.S. Cole, the train bombings in Madrid and the attack on the school in Beslan demonstrate the willingness of terrorists to use every available weapon -- even very sophisticated and advanced weapons -- to

achieve their goal. We cannot accept the NRC arbitrarily removing potent weapons from the design basis threat assessment to satisfy industry objections.

Another key element of any security plan is the need for periodic testing to determine the continued effectiveness of the overall system. Unfortunately, the testing of security at nuclear power stations is so unrealistic as to be nearly meaningless. It has been described as a farce by some experts, and as questionable by the GAO.

The current NRC guidelines require periodic "force on force" exercises, designed to imitate an actual attack to be met and repelled by the plant's security teams. There are several major flaws in the current system.

The "attacking force" in every exercise has been undersized, in part because of mistaken assumptions about the attacking force. A more realistic assumption is that some or all of the attackers will be suicide bombers, including individuals dressed as plant workers, visitors, or even police (all tactics used by existing terrorists), carrying explosive vests or driving bomb-laden trucks. Multiple attacks on nearby public buildings and roadside bombs designed to impede or divert responding police or National Guard troops should also be included in the scenarios.

An even more basic flaw exists in the current testing system: The same company that protects the plants provides the attacking teams, and all of the "defenders" are notified of the "surprise" attack well beforehand. This approach gravely undermines the validity of the training tests.

Spent Fuel Pools

Most of the radioactive material at the nation's 103 power stations is contained in spent fuel pools, not in the reactors. Once a certain amount of the uranium in the fuel rods has passed its half-life and decayed so that it is no longer usable as fuel, the rods are removed from the reactor and placed in a water-filled spent fuel pool to cool down. While no longer suitable for use as fuel, the rods remain highly radioactive. Lacking a central repository, these fuel rods have accumulated in the pools -- in some cases for decades. Consequently, most power plants have several times as much radioactive material in the fuel pools as in the reactors.

From a security perspective, there are two problems. The first relates to storage separated from reactors, which are almost universally housed in thick steel reinforced concrete containment domes. These domes are hardened massive bunkers that can resist most explosive attacks, but most of the dangerous radioactive material is stored outside the containment domes, in far more accessible and less protected fuel pools.

In fact, most such spent fuel pools are effectively comparable to large swimming pools covered by a simple steel industrial building. These structures are exceedingly vulnerable to truck bombs or even smaller explosives. Relatively slight damage to a fuel pool may result in release of radioisotopes.

If a pool is breached, a loss of cooling water will lead quickly to a buildup of heat from the fuel rods. This heat, if not abated, will cause the cladding on the rods to ignite. The resulting fire will release radioactive uranium in the form of radioactive dust rising on the heat plume. Thus, an attacking force may generate a cloud of radioactive fallout by over-coming outer plant security and breaching the highly vulnerable fuel pool. Other well-established terrorist tactics include the use of booby-traps or improvised explosive devices (IEDs) left behind to hinder response efforts.

The design basis threat assessment should be amended to ensure adequate assessment of the risk of attacks on the spent fuel pools.

Air Exclusion Zone

Security for a nuclear power plant must include more than armed guards and a perimeter fence. The NRC must seriously consider attacks from the air. While the Commission has stated that existing containment domes can resist impacts from airliners, this view must be reevaluated. Specifically, NRC has traditionally relied on a decades old analysis of the potential impact from a Boeing 707 airliner. Many newer aircraft are much larger and heavier. Congress should compel the NRC to reexamine the issue of whether 30 year old concrete containment domes can resist an impact from the current generation of aircraft.

The NRC should also establish an air-exclusion zone. As I have repeatedly raised with the NRC, if Disney World merits a no-fly zone, a similar aircraft exclusion zone should be required for nuclear power stations.

The NRC needs to think broadly, perhaps outside the box, about security threats -- thinking the unthinkable. At a recent NRC annual assessment hearing on the Millstone Nuclear Power Plant, I urged the NRC to consider additional threats from liquefied natural gas (LNG) tankers that would pass near the plant -- located directly on Long Island Sound -- as part of the proposed Broadwater project. These LNG tankers can carry up to 250,000 cubic feet of liquid methane -- a cargo so flammable that the Coast Guard is currently investigating how large a security zone must surround the tankers to protect the public from the massive conflagration that could be caused by an attack or accident.

In summary, our nation's nuclear power facilities are dangerously vulnerable. Congress should move the NRC to act far more effectively and decisively to protect those plants, and all Americans, from a possible terrorist attack.

I urge this committee to act forcefully and expeditiously.

Mr. SHAYS. I thank the gentleman very much. And frankly, I wish I had gotten into the issue of spent fuel, particularly with the Commission because I do agree with you. It is a good way to describe it, being like a house for a swimming pool.

Ms. Brian.

STATEMENT OF DANIELLE BRIAN

Ms. BRIAN. Chairman Shays, thank you for inviting POGO to testify at this important hearing. It's clear you share many of the same priorities as POGO across the board—security at nuclear power plants and at the nuclear weapons complex, excessive Government secrecy, whistleblower protections. I think your subcommittee is doing the most important work in the Congress, and I think it's important to recognize that. And you're not my Congressman.

The GAO report that you Commissioned is shocking and confirms what POGO has been alarmed about for the past 3 years. It detailed the inappropriate influence of the nuclear industry on the NRC's design basis threat process. They essentially get two bites of the apple.

The nuclear industry is allowed to lobby the NRC security staff to lower the security standards recommended to the Commission, and then the NRC Commissioners removed weapons that were recommended despite that lobbying, including what we understand included the two weapons in question were RPGs and 50-caliber rifles with armor-piercing rounds. Because industry claimed it was too expensive for them to protect against such a threat.

The result of this process is a completely unrealistic DBT that reflects not what intelligence estimates dictate, but instead what industry is willing to pay for. Because of the lowering of these security standards, at one site the GAO found some or all of the attackers during the force-on-force were able to enter the protected area in each of the three exercise scenarios.

At another, the mock attackers were able to destroy three out of four targeted components. At another site, they didn't even include spent fuel pools among the targets to be protected.

It should be understood these failures occurred even though there remain significant artificialities in the tests in the first place. They are still scheduled and announced 8 to 12 weeks before they occur, giving the security force ample time to prepare. Furthermore, the GAO found the security force can tell within minutes at what time the test will begin.

Counter to what we were hearing in the last panel, while I certainly agree these tests are far better than they were when we first started talking about this a few years ago, the GAO also found that the controllers, who are essentially the referees in these tests, were sometimes volunteers from the plant, just like we had seen before, who had no security experience at all. And they're the people who essentially get to decide who was living or dying in a particular exchange.

At approximately half the sites, the mock attackers and security force they are testing are employed by the same company, Wackenhut. Whether those tests are honest or not, how can the

public have faith in a system with such an obvious conflict of interest?

Even with these weaknesses, the GAO also found evidence of behavior that some might call cheating. In one case, a site employee made motions that may have alerted the security officers to the targets the adversaries would be trying to reach that evening. Now imagine, these are the tests where they know the GAO is watching them.

Just last year, several years after the September 11th attacks, NBC News asked the Nuclear Energy Institute spokesman about Mohammed Atta's plans to target what is now believed to have been Indian Point. His reaction? He said he'd never heard of Mohammed Atta.

The impact of this ostrich-like approach to the homeland security needs of our country permeates the nuclear community, both the industry and its regulator, the NRC. Perhaps the most important evidence that the NRC remains in denial is their decision to require nuclear power plants to protect only against a handful of terrorists. This decision is based on the assumption that only one terrorist cell acting alone would attack the plant.

There is no explanation why the NRC continues to come to this conclusion, despite historical evidence that multiple cells of terrorists were used collectively on September 11th. The GAO points out that the Department of Energy, an agency which we've both had some problems with as well, but they still do a lot better on this than the NRC has. They're relying on the same intelligence as the NRC when determining their DBT.

In comparison, however, the DOE requires their facilities to protect against an attacking force about three times that required by the NRC and against the very weapons rejected by the NRC. Their security is also provided by a private force. I think it's important to dispel the myth that private forces can't be asked to do more than they are. The difference, however, in the two agencies' processes is that the DOE does not have an industry lobbying them to lower their standards.

It's important to recognize the two steps—as you said before, so I won't repeat them—that there essentially is the threat assessment staff and then the Commission that is reducing the weapons. But the thing that really alarms us is that these RPGs that are of particular concern to us are very available.

As we wrote to Commissioner Diaz on February 22nd, we raised our concerns that the Commission decided not to protect, we believe, against these weapons. Despite the fact that during a special forces mission in West Africa last year, Pentagon officials found that an RPG could be purchased for less than $10 on the weapons market and were available in large quantities in a matter of hours.

This is equally true in South Asia. Pentagon officials have told POGO that getting shipments of RPGs into the United States would be surprisingly easy.

I wanted to emphasize a final quote from the GAO that removal of these weapons from the revised DBT was significant because of the strength of the NRC staff's intelligence analysis supporting their inclusion. I'd like to include a copy of the letter we wrote to Chairman Diaz with our concerns about this.

It's also important to recognize that this is a problem that's easy to fix. In an unclassified film created by the Department of Energy named "Systems Under Fire," they outline the relative ease with which RPGs can destroy traditional barriers. They also show a relatively inexpensive defensive measure, predetonation screens, that the industry should be required to adopt, which would effectively mitigate the lethality of these weapons.

The NRC Commissioners watered down the original staff proposed security standards based on the belief they can only ask of the nuclear industry what can be expected of a private security force, but we really believe this is backward logic.

Security professionals should determine the security threat and then determine what is required to meet that threat. If it is concluded that private forces cannot adequately protect the facilities to the standards set by the intelligence community, then it is the Government's job to step in at industry's expense.

Mr. SHAYS. We did a second round. I think we need to close you down here in a second.

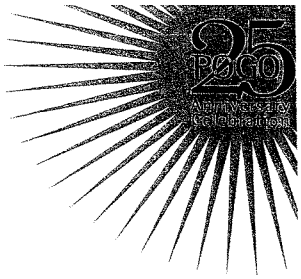
Ms. BRIAN. Yes. I can——

Mr. SHAYS. That is a term that the—"close you down" is not a good term.

Ms. BRIAN. OK. I'll just conclude by saying our concern is that there is no one accepting the responsibility of making that leap between the DBT and what is actually required. I want to point out that I have great respect for a lot of the security staff at the NRC and Commissioner McGaffigan in particular. And I think they're coming at this with really honest efforts, but it's tremendous pressure that they're receiving as well.

[The prepared statement of Ms. Brian follows:]

Project On Government Oversight
Exposing Corruption Exploring Solutions www.POGO.org



Testimony of
Danielle Brian,
Executive Director
Project On Government Oversight
(POGO)
before the
House Subcommittee on National Security,
Emerging Threats, and International Relations
on
Nuclear Security:
Has the NRC Strengthened
Facility Standards Since 9/11?

April 4, 2006

www.POGO.org

Chairman Shays, thank you for inviting POGO to testify at this important hearing. It is clear you share many of the same priorities as POGO: security at nuclear power plants and at the nuclear weapons complex, excessive government secrecy, and whistleblower protections. Your Subcommittee is doing the most important oversight work in the Congress.

The Government Accountability Office (GAO) report that you commissioned, "Efforts Made To Upgrade Security, but the Nuclear Regulatory Commission's Design Basis Threat Process Should be Improved" (GAO-06-388), is shocking and confirms what POGO has been alarmed about for the past three years. It details the inappropriate influence of the nuclear industry on the Nuclear Regulatory Commission (NRC)'s Design Basis Threat[1] process:

- The nuclear industry is allowed to lobby the NRC security staff to lower the security standards recommended to the Commission; and

- The NRC Commissioners removed commonly-used weapons from the DBT, including RPGs, 50-caliber rifles with armor-piercing rounds, and other weapons. They also reduced the size of the truck bomb necessary to defend against, and minimized the impact of an active insider helping the terrorists, because industry claimed it was too expensive for them to protect against such a threat.

The result of this process is a completely unrealistic DBT that reflects not what intelligence estimates dictate but, instead, what industry is willing to pay for. Because of the lowering of these security standards:

- At one site where the GAO observed force-on-force tests, "the site's ability to defend against the DBT was at best questionable ... . Some or all of the attackers were able to enter the protected area in each of the three exercise scenarios. Furthermore, attackers made it to the targets in two of the scenarios ... ." (pp. 40-41)

- At one site, the mock attackers "were able to destroy three out of four targeted components ... ." (p. 57)

- At one site, a site had not included the control room or spent fuel pool among its targets. (p. 58)

- Two-thirds of the NRC security inspection reports and nearly 50% of the force-on-force inspection reports "identified problems or items needing correction." (p. 40)

---

[1] The Design Basis Threat (DBT) describes the level of threat the protective force is required to defend against – the number of outside attackers and inside conspirators, and the kinds of weapons and size of truck bombs that would be available to terrorists.

It should be understood that there remain significant artificialities in the NRC's security tests:

- In a real terrorist attack, the terrorists would have three major advantages: speed, surprise and violence of action. Not one of these are tested in force-on-force tests;

- These tests are still scheduled and announced 8 to 12 weeks before they occur – giving the security force ample time to prepare. Furthermore, the GAO found that the security force can tell within minutes at what time the test will begin;

- The referees, or controllers used for these tests, whose task is to determine who "lives" and who "dies" were sometimes volunteers from the plant with no security experience at all;

- At approximately half the sites, the mock attackers and the security force they are testing are employed by the same company, Wackenhut. How can the public have faith in a system with such an obvious conflict of interest?

- Even with these weaknesses, the GAO also found evidence of behavior that some might call cheating. The GAO wrote that during one test it observed:

> ... a lapse in protection of information about the planned scenario for a mock attack that we observed may have given the plant's security officers knowledge that allowed them to perform better than they otherwise would have ... . (p. 9) For example, during a safety "walk down" ... a site employee made motions that may have alerted security officers to the targets the adversaries would be trying to reach that evening. (p. 45)

Imagine. This is happening on a test they KNOW is being audited by the GAO.

Why is this important? As the GAO pointed out, the 9/11 Commission confirmed that "nuclear power plants were among the targets considered in the original plan for the September 11, 2001, attacks." I suspect that is not news to the members or staff of this committee. What might surprise you though, is this: Just last year, several years after the 9/11 attacks, NBC News asked the Nuclear Energy Institute spokesman about Mohammed Atta's plans to target what is now believed to have been Indian Point. His reaction? He said he had never heard of Mohammed Atta. The impact of this ostrich-like approach to the homeland security needs of our country permeates the nuclear community – both the industry and its captured regulator, the NRC.

Perhaps the most important evidence that the NRC remains in denial is their decision to require nuclear power plants to protect against a only handful of terrorists. This decision is based on the assumption that only one terrorist cell, acting alone, would attack a plant. The GAO explains that the NRC believes "multiple cells along the lines of the September 11, 2001, attacks would not *necessarily* target a single nuclear power plant" and therefore the plants do not need to

protect against more than a handful of attackers. [emphasis added] There is no explanation why the NRC comes to this conclusion, despite historical evidence that multiple cells of terrorists were used collectively on 9/11. Inexplicably, the NRC is confident they do not need to require nuclear power plants to be protected against a similarly-sized attack. The GAO points out that the Department of Energy (DOE) relied on the same intelligence as the NRC when determining their DBT. In comparison, the DOE requires their facilities to protect against an attacking force THREE TIMES that required by the NRC, and against the weapons rejected by the NRC – and their security is also provided by a private force. The difference in the two agencies' processes is that the DOE does not have an industry lobbying them to lower their standards.

The GAO relates the NRC's conclusion that it is not valid to compare NRC and DOE sites. The NRC argues that terrorists attacking a DOE nuclear weapons facility would be more heavily armed because they have to get both into and back out of a facility with a nuclear weapon or Special Nuclear Materials, while they argue terrorists attacking a nuclear power plant would be suicidal in their attempt at radiological sabotage. As you know Mr. Chairman, this is ill-informed. The biggest threat to DOE facilities is a suicidal attack to detonate an improvised nuclear device (an actual nuclear detonation) without the intent to come back out alive. Therefore, while the consequences of an attack on a DOE facility may be far greater than at a nuclear power plant, there is no reason to believe the terrorists would come more heavily-armed or in greater numbers than when attacking a nuclear power plant. Security analysts believe a serious terrorist attack on a nuclear plant would involve no less than a "squad size" of adversaries (12 personnel for U.S. Army Special Forces; 14 personnel for Navy SEALs).

In addition to requiring nuclear plants to protect against only a handful of attackers, the NRC's DBT also continues to turn a blind eye to protecting against weapons well-known to be used by terrorists around the world.

The GAO reveals a shocking level of influence by the nuclear industry during the NRC's process of determining these security requirements. The report reveals that the industry essentially gets two opportunities to lobby the NRC to water down its security requirements. First, industry is consulted by the NRC's Threat Assessment staff. As the GAO wrote:

> A number of the changes [to its initial recommendations] reflected industry objections to the draft. For example, following meetings with industry, the staff decided not to recommend including certain weapons in the list of adversary characteristics that nuclear power plants should be prepared to defend against. In its comments, the industry had pressed for NRC to remove such adversary characteristics from the draft DBT. The industry considered these adversary characteristics prohibitively expensive to defend against .... [I]n our view the process by which NRC used the threat assessment staff to obtain stakeholder feedback created the appearance that changes were made based on what industry considered reasonable and feasible to defend against rather than an assessment of the terrorist threat, especially given the high degree of judgment involved in assessing threat information. (pp. 6-7)

Even after this process, the NRC Commissioners voted to remove two more weapons from the list of weapons the plants must protect against, with no countermanding intelligence to justify the change. POGO wrote to NRC Chairman Diaz on February 22, 2006, raising our concerns about the 3-1 vote by the Commission to overrule the professional security staff, and to not require the utilities to protect the plants against the use of certain lethal weapons, including rocket-propelled grenades and 50-caliber rifles with API rounds. POGO wrote, "During a Special Forces mission in West Africa last year, Pentagon officials found that an RPG-4 could be purchased for less than $10 U.S. on the weapons market, and were available in large quantities in a matter of hours. This is equally true in South Asia. Pentagon officials have told POGO that getting shipments of RPG's into the U.S. would be surprisingly easy." As the GAO described, "[R]emoval of weapons from the revised DBT was significant because of the strength of the NRC staff's intelligence analysis supporting their inclusion." (p. 27) I'd like to submit POGO's letter to Chairman Diaz for the record.

NRC Commissioners watered down the original staff-proposed security standards based on the belief that they can only ask of the nuclear industry what can be expected of a private security force. POGO believes this is backwards logic. Security professionals should determine the security threat, and then determine what is required to meet that threat. If it is concluded that private forces cannot adequately protect the facilities to the standards set by the intelligence community, then it is the government's job to step in, at industry's expense, to figure out how to meet that threat. Currently, no one is accepting this responsibility.

This dichotomy – between the threat and standards required by the NRC – all comes down to money. This is not a debate over what the intelligence community believes, it is a debate over how much the nuclear industry should have to pay. As the GAO pointed out:

> NEI argued against the inclusion of a number of weapons. For example, NEI wrote that (1) one particular weapon recommended by the NRC staff would render the ballistic shielding used at nuclear power plants obsolete ... .

The significance of this point is that the nuclear industry is claiming they don't want to have to protect against 50-caliber rifles (which have been around since World War I) with armor-piercing rounds because they would then have to acknowledge that their bullet-resistant enclosures can not protect against these weapons. As a result, one of their primary defensive measures – ballistic shielding around these enclosures – would be rendered useless. So rather than addressing the potential vulnerability, the NRC – at NEI's behest – caved in and pretended these widely-available weapons and ammunition do not exist in their world.

To continue, the GAO found that:

> ... (2) another proposed weapon would initially cost $1 million to $7 million per site to defend against, with annual recurring costs of up to $2 million per site ... . In the final draft submitted to the NRC commissioners, the NRC staff removed a number of weapons

> NEI had objected to. . . . The NRC staff did not remove one particular weapon NEI had objected to, which, according to NRC's analysis, has been a staple in the terrorist arsenal since the 1970s and has been used extensively worldwide .... [T]he NRC commissioners later voted to remove this particular weapon.

We believe this weapon to be rocket-propelled grenades (RPGs). In an unclassified film created by the DOE, "Systems Under Fire," they outline the relative ease with which RPGs can destroy traditional shielding. They also show a relatively inexpensive defensive measure – pre-detonation screens – that the industry should be required to adopt which would effectively mitigate the lethality of these weapons.

The NRC continues to operate under a 1967 policy that the nuclear industry is not responsible for protecting the plants against "enemies of the state," including airborne attacks. This policy was formed because of a concern that Cuba might attack a Florida nuclear power plant. This paradigm is entirely out of date. It is clear that Al Queda is at least as capable of generating as large an attack as Cuba. But more practically, what does this distinction mean? Are security officers expected to demand passports from attackers as they flood through the fence? If it is determined that the attackers are "enemies of the state," how long will it take for outside law enforcement to get there? DOE timelines suggest it will take approximately 1 ½ to two hours for SWAT teams to be assembled, gather their equipment and weapons, be transported to the site, get briefed on the status of the attack, and engage. The problem is that these attacks are expected to take between three to eight minutes before they are won or lost. If the private security force isn't responsible for handling such an attack, who will be there to take on that responsibility and protect the public from the consequences of a terrorist attack?

The GAO's findings clearly reveal devastating discrepancies between current security standards at nuclear power plants and what is needed to repel a terrorist attack. It is clear that the public can not trust the combined efforts of the nuclear industry and the Nuclear Regulatory Commission to protect the them.

February 22, 2006

POGO's letter to Nuclear Regulatory Commission Chairman Diaz on the proposed Design Basis Threat (DBT)

February 22, 2006

Annette Vietti-Cook, Secretary
U.S. Nuclear Regulatory Commission
11555 Rockville Pike
Rockville, MD 20852

Attn: Rulemaking and Adjudications Staff

Chairman Nils J. Diaz
U.S. Nuclear Regulatory Commission
11555 Rockville Pike
Rockville, MD 20852

Re: RIN 3150- AH60, Proposed Rule 70 FR 76,380 "Design Basis Threat"

Via email to SECY@nrc.gov and
Via facsimile: (301) 415-1757

Dear Chairman Diaz,

I understand you intend to leave the Chairmanship of the Nuclear Regulatory Commission (NRC) this year. I also understand that you would like to leave behind a lasting legacy. I am taking advantage of the current rulemaking process to write to you about what is, without exception, the single most important matter entrusted to you by the American public – the federal government's security standards for the nation's nuclear power plants.

As you know, the Design Basis Threat (DBT) is the bedrock of the NRC's security posture. It includes the number of adversaries, the weapons they are likely to use, and the size of the truck bomb against which a nuclear power plant must defend. Prior to 9/11, the number of adversaries against whom nuclear power plants had to guard was a pathetic three. Two years after the 9/11 attacks involving 19 terrorists, the Commission only raised the security requirements to protecting against five terrorists – a paltry response to what we have learned about the capabilities and tactics of terrorists from the 9/11 attack and other terrorist attacks around the world. (Interestingly, air attacks are still not seriously addressed in the DBT.)

During my 2004 address at the NRC's annual Regulatory Information Conference, I argued that a serious terrorist attack on a nuclear plant would involve no less than a "squad size" of adversaries (12 personnel for US Army Special Forces; 14 personnel for Navy SEALs). Our sources on this recommendation are Army Special Operations, Navy SEALs, Pentagon, and Defense Threat Reduction Agency (DTRA) personnel. I also argued that terrorists would bring far more lethal weapons than are included in the NRC DBT. I pointed to a Department of Energy (DOE) film – "Systems Under Fire" – which demonstrates the types and lethality of the weapons available to and regularly used by terrorists. Rather than focusing on the substance of the DOE's findings and upgrading the NRC's security requirements accordingly, NRC Commissioners met on more than one occasion with the Deputy Secretary of DOE arguing that the film should be classified.

The NRC's DBT baseline is counter-intuitive. Instead of sizing the DBT on the actual threat, the NRC bases security standards on what the NRC (or perhaps the nuclear industry) believes a private guard force can be expected to handle. You wrote in the June 2005 rule-making on the DBT that, "The DBT is based on actual demonstrated adversary characteristics and a determination as to those characteristics ***against which a private guard force could reasonably be expected to provide protection***." [emphasis added] Yet surely you are aware that DOE nuclear weapons facilities are also protected by private guard forces, and are expected to handle a DBT more than three times the level of the NRC's. The NRC's security standards should be based on security needs, not the financial impact on private industry. The NRC must better articulate what, exactly, is too much for a private security force to be expected to handle. The lack of specificity on this question is allowing basic threats to be utterly ignored.

The corollary problem is the hollow assurance made by the NRC that outside credible SWAT capability will arrive and take over from private security forces at the point where they are no longer capable of or responsible for to protecting the plant or surrounding community. It is unrealistic to believe that the nuclear plants can depend on outside help to defeat a terrorist attack. The consensus among those security experts consulted by POGO is that a suicidal attack on a nuclear plant aimed at the reactor or spent fuel pools would be finished, one way or the other, in 3-10 minutes. I am sure you're aware that it will take between 1 ½ to 2 hours for outside law enforcement help to arrive, be briefed on the status of the attack, communicate with what is left of the guard force, and engage in battle – long after the battle would have been over.

POGO has an unclassified list of the weapons that Department of Homeland Security experts believe would be used by adversaries in the event of an attack on a nuclear facility. However, we understand that many of these weapons are not in the NRC DBT. We have reason to believe that the NRC's security staff recommended to the Commissioners that nuclear power plants be prepared to protect against Rocket-Propelled Grenade (RPG) attacks – but the Commission recently voted against this sensible security requirement in a 3-1 vote. During a Special Forces mission in West Africa last year, Pentagon officials found that an RPG-4 could be purchased for less than $10 U.S. on the weapons market, and were available in large quantities in a matter of hours. This is equally true in South Asia. Pentagon officials have told POGO that getting shipments of RPG's into the U.S. would be surprisingly easy. If it is true that RPG's have not been included in the NRC's DBT, there is simply no excuse for it. As can be seen in the Department of Energy's unclassified movie, "Systems Under Fire," there are readily-available and low-cost means of defeating these weapons such as pre-detonation screens.

We also understand that the Commission has voted down the staff's recommendation to require nuclear power plant security to protect against a number of other common lethal weapons – including ones that have been around for close to 100 years and others currently being used by terrorists around the world. These weapons include bangalore torpedoes which will blow apart a double fence in a few seconds; platter charges that travel at 6000 feet per second and will penetrate at least six feet of reinforced concrete because it imparts millions of foot pounds of energy; and 50 caliber Armor-Piercing Incendiary (API) rounds.

As you know, it would only take terrorists 45 seconds to get from the alarmed double-fence line into many of the Pressurized Water Reactors spent fuel pools. And it would only take minutes to blow a hole in the bottom of the pool with one of these explosives, creating what the National Academy of Sciences describes as potential serious release of radiation. We have consulted a variety of experts, such as a national guardsman with special operations training who was called up after 9/11 to protect an East Coast nuclear power plant. After some assessment, he told POGO that, with a .50 caliber rifle with API rounds from a single location outside the facility's perimeter, he could have easily destroyed most of the Bullet Resistant Enclosure guard towers. Many of the plants' security officers refer to these towers as "iron coffins." DOE has ceased using even state-of-the-art guard towers because of their vulnerability, yet nuclear plant licensees are relying on them more frequently.

Finally, the NRC needs to upgrade its stewardship of highly-enriched uranium (HEU), at Nuclear Fuel Services in Erwin, Tennessee, and the Nuclear Products Division of BWXT in Lynchburg, Virginia, as well as at university research reactors that use HEU. There is no reason why the Erwin and Lynchburg facilities should have a DBT any less than DOE requires of its Category I (weapons quantities of weapons-grade material) facilities. While university research reactors may not individually contain enough HEU to make a bomb, a combination of two university reactors could. HEU is, without question, a terrorist's weapon of choice. It is the easiest ingredient to use to make an Improvised Nuclear Device (a crude nuclear bomb), which could be as large as 10-kilotons – one that has the same yield as the nuclear bomb used on Hiroshima. As a result, securing all sources of HEU must be given the government's top priority.

POGO's concerns regarding the NRC's inadequate DBT are not alarmist, and are based on real threats. As the 9/11 Commission confirmed, terrorists have considered targeting nuclear power plants in the past, including Indian Point which is less than 50 miles from New York City. In fact, in his 2002 State of the Union Address, President Bush confirmed that U.S. forces "found diagrams of American nuclear power plants" in caves used by al-Qaeda in Afghanistan.

Clearly, the Attorneys General from New York, Connecticut, Illinois, Arkansas, Arizona, and Wisconsin – states that are home to numerous nuclear power plants – do not believe that the NRC's DBT is adequate. As they urged the NRC in January 2005, "amend [federal regulations] to require nuclear power plant owners to prepare to repel air, water or land assaults by a group at least as large as the 19 terrorists who acted on 9/11, attacking at more than one point at the same time and using any appropriate weapons, means of sabotage and vehicles."

If there is an attack on a nuclear plant with the weapons and tactics described – weapons and tactics against which the Commission decided were not important to defend – NRC records will reveal to the public exactly who on the Commission dismissed the actual threat the professionals knew existed. Something to consider.

POGO continues to request a meeting with you in order to discuss a range of issues that concern us. We believe the NRC is abdicating its responsibility to the public and needs to make significant improvements right away. I look forward to your response.

Sincerely,

Danielle Brian
Executive Director

Mr. SHAYS. Right. Thank you very much.
I am hoping I can hear everyone testify before I have to go.
Mr. Fertel.

STATEMENT OF MARVIN FERTEL

Mr. FERTEL. Thank you, Chairman Shays, members of the subcommittee.

In my testimony today, I would like to make three points. First, the growing need for electricity supply, energy security, and the concern over global warming has led to a resurgence of the interest in nuclear energy.

Second, in response to the question, are our Nation's nuclear plants more secure than they were before September 11th? I would say the answer is a resounding yes, and I think the GAO actually says that, too. Over the past 4 1/2 years, the industry has made substantial and significant improvements to an already-strong security.

Finally, the nuclear energy industry recognizes that the spectrum of possible threats facing the Nation can be larger than the NRC's design basis threat for nuclear power plants. And because of that, we've led efforts, under the auspices of the Department of Homeland Security, to assess the potential vulnerabilities of our critical infrastructure to a broader spectrum of threats and to coordinate Federal, State, and local resources to complement and supplement plant security in the face of such threats.

With regard to my first point, according to the projections from the U.S. Energy Information Administration, even with a strong commitment to efficiency and conservation, our Nation is expected to need 45 percent more electricity by 2030. Much of this new electricity supply will be needed in the form of large-scale baseload generation. The only realistic alternatives to significantly increasing baseload generation are coal and nuclear energy.

The Congress recognized the need for a diverse energy portfolio and the importance of nuclear in that portfolio in the Energy Policy Act of 2005. That bill is having its intended impact. Nine companies are pursuing actions toward building between 12 and 19 new nuclear plants in the United States, and we expect that the new nuclear power plants will become operational within about a decade.

Let me turn now to security. When I was here just over 18 months ago, I testified that nuclear power plants are the most secure commercially owned facilities in the country. That remains true today because we have continued to work to meet the NRC requirements, satisfy our own performance expectations, and most importantly, through DHS, enhance integration with Federal, State, and local authorities responsible for providing security to our Nation's critical infrastructure.

Specifically, over the past 4 1/2 years, we have improved our security in several steps. The first step was what the Commission talked about that occurred on September 11th. Just 4 months later, in February 2002, the NRC again increased security requirements in several areas.

The industry, complying with the NRC orders, instituted additional measures, such as extending or fortifying security perim-

eters, increasing patrols within security zones, installing new barriers to protect against vehicle bombs, installing additional high-tech surveillance equipment, and strengthening security coordination with local, State, and Federal agencies.

Following the completion of its top-to-bottom review and its study of the potential threats to nuclear power plants, the NRC issued three orders in April 2003. One order revised the DBT, further increasing plant security requirements.

In addition to modifying the DBT, the NRC also issued orders that enhanced training and qualifications for security officers and improved access control and established work hour limits. We estimate the cost across our 64 sites of this additional security since 2001 is now over $1.2 billion.

Since the September 2004 hearing before this subcommittee, we have implemented NRC's approved security plans at each site. We've completed the physical improvements at each site as required by the DBT defined by the NRC.

We've conducted 27 NRC-observed force-on-force drills, and we can play with those numbers if they are still confusing, and also hundreds of such drills as part of the industry's programmatic security training program. We've been a national leader working with the Department of Homeland Security by completing 22 risk assessments and 20 comprehensive reviews for nuclear power plants.

Given all we have done and although the GAO identified some areas for improvement, we are very pleased that GAO also agrees with what the industry has been saying; that nuclear power plants have made substantial security improvements after September 11th.

As my final point, I want to emphasize that security at nuclear power plants does not end with what the NRC requires, nor with what plant operators can provide to protect our Nation's critical infrastructure. Industrial and commercial facilities must integrate their security with local, State, and Federal forces. The industry recognizes that there is a spectrum of potential threat; some less, some greater than the capabilities of our or any other private sector plant security program.

Recognizing this fact, the industry has provided national leadership and is the first industrial sector to participate in the Department of Homeland Security's Risk Assessment and Management for Critical Asset Protection [RAMCAP] program and its comprehensive review program. Twenty-two sites have gone through RAMCAP, and 20 nuclear plant sites have already completed the comprehensive reviews. We expect to complete all of them by July 2007.

These DHS programs represent areas where significant enhancements to security can be achieved for nuclear plants and for all the other sectors of the critical infrastructure. This subcommittee can be instrumental in furthering programs like this, and we would encourage the subcommittee to support DHS in its effort to complete these activities for the entire critical infrastructure.

In closing, we are pleased that the GAO agrees that our security has been greatly improved. We look forward to fulfilling our responsibilities and continuing to work with governmental agencies, such as GAO, DHS, and the NRC, as well as Congress, to ensure

that our facilities remain the most secure facilities in the Nation's critical infrastructure.

Thank you.

[The prepared statement of Mr. Fertel follows:]

TESTIMONY OF

MARVIN FERTEL
SENIOR VICE PRESIDENT AND CHIEF NUCLEAR OFFICER
NUCLEAR ENERGY INSTITUTE

BEFORE THE
NATIONAL SECURITY, EMERGING THREATS
AND INTERNATIONAL RELATIONS SUBCOMMITTEE

COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

APRIL 4, 2006

Chairman Christopher Shays, Ranking Member Dennis Kucinich and distinguished members of the subcommittee, I am Marvin Fertel, senior vice president and chief nuclear officer at the Nuclear Energy Institute (NEI). I am honored to address the issues before this subcommittee today. As in previous years, I am here to discuss the importance of nuclear energy for our nation's economic growth and energy security. The nuclear energy industry is a leader in the area of industrial security and, as the committee requested, I will address how the industry has secured nuclear power facilities as deemed necessary by plant management and required by the U.S. Nuclear Regulatory Commission.

NEI is responsible for developing policy for the commercial nuclear industry. NEI's 250 members represent a broad spectrum of interests, including every U.S. electric company that operates a nuclear power plant. NEI's membership also includes nuclear fuel cycle companies, suppliers, engineering and consulting firms, national research laboratories, manufacturers of radiopharmaceuticals, universities, labor unions and law firms.

America's nuclear facilities maintained extremely high levels of security prior to Sept. 11, 2001, and that security is even better today. However, the nuclear energy industry continues to improve security at our nuclear power plants, and we are constantly assessing and testing our security programs.

Security at our nuclear power plants is a shared responsibility. The industry believes the greatest enhancements in security around nuclear plant sites will come by developing comprehensive strategies that combine our security and emergency planning resources with those of local, state and federal entities.

The industry is pleased that the Government Accountability Office has recognized the many improvements the industry has made since Sept. 11 and in response to increased Nuclear Regulatory Commission requirements. The GAO also noted the improvements to the force-on-force security exercises that are uniquely used by the nuclear industry to test our security programs and systems. The industry has implemented most of the GAO's recommendations in this area. We will continue to working with Congress and government agencies to address emerging issues.

My testimony will address the following four issues:

- Growing electricity demand and concern over energy security and climate change has led to a resurgence of interest in nuclear energy. The Energy Policy Act of 2005, signed into law by President Bush and passed with broad bipartisan support in both branches of Congress, has added to an already increasing interest in the construction of new nuclear plants.

- Clearly, the nation's nuclear power plants are more secure today than they were before the Sept. 11 terrorists attacks. America's commercial nuclear power plants have long been considered the most secure facilities in our nation's critical infrastructure. Since 2001, the nuclear energy industry has made these facilities even more secure. Over the past four years, the NRC elevated nuclear facility security requirements numerous times by issuing orders and other formal requirements, and the agency is in the process of codifying additional requirements in rulemakings. The industry has invested more than $1.2 billion in security improvements at nuclear plant sites and has increased the number of specially trained, well-armed security forces by more than 60 percent.

- Since I last testified before this subcommittee in 2004, the industry has taken these broad actions to enhance security for our workers and our neighbors in the communities in which we operate nuclear power plants:

  - implemented NRC-approved security plans for each nuclear power plant
  - completed physical security improvements required by the NRC
  - conducted hundreds of force-on-force security exercises at 64 plants, including NRC-observed and -supervised force-on-force drills at 32 plant sites
  - implementing enhanced security provisions in the Energy Policy Act of 2005, in coordination with the NRC
  - completed more than 20 Department of Homeland Security comprehensive reviews of nuclear power plants.

- The nuclear energy industry recognizes that the spectrum of possible threats facing a nation can be larger than the design basis threat for a nuclear power plant. The design basis threat (DBT) defines the abilities of a potential attacking force against which the industry's security strategy must succeed. The industry has been a private sector leader, working under the auspices of the Department of Homeland Security, to assess a broader spectrum of threats to the nation's critical infrastructure. These assessments will help DHS decide how best to allocate federal and state resources to supplement private security forces at each plant site. Security at nuclear power plants provides a solid basis from which this more integrated federal, state, local and private response can be built. When the NRC elevated the DBT for nuclear power plants, it appropriately considered both the threats facing our nation, and the policy, legal and practical limitations on a private entity in facing these threats.

NUCLEAR POWER PLANTS ARE ESSENTIAL TO U.S. ENERGY SECURITY

Prior to discussing how the industry ensures that our plants remain secure, it is important to emphasize the importance of nuclear energy to a diverse electric portfolio that helps maintain economic growth and our quality of life. Economic growth and quality of life are closely linked to affordable, abundant electricity.

Nuclear energy is a vital part of our nation's diverse energy portfolio, safely and cleanly producing electricity for one of every five U.S. homes and businesses. The United States remains the world leader in nuclear energy, with 103 reactors generating 783 billion kilowatt-hours of electricity in 2005—more than *all* of the electricity used in France and the United Kingdom combined. Nuclear energy is the United States' only large-scale source of electricity that is readily expandable and does not produce greenhouse gases. The industry's exemplary safety record and reliability, low operating costs and future price stability make nuclear energy a vital source of electricity today and for the future.

Coal and nuclear energy represent 70 percent of our electricity supply today. Since 1992, the electric industry has built more than 275,000 megawatts of natural gas-fired power plants, but has added only 14,000 megawatts of new nuclear and coal-fired capacity. All of those baseload power projects started construction in the 1980s. We are now suffering the consequences of relying too heavily upon one fuel for electricity production. Although electricity prices on the whole have increased far less than the prices of other consumer goods during the past two decades, high natural gas prices have caused dramatic electricity price increases in many regions during the past year. Natural gas also is a critical feedstock for other industries, such as chemical plants. The chemical industry has lost $50 billion in business to overseas operations since 2000, closed 100 chemical plants and laid off more than 100,000 workers.

Even with a strong commitment to efficiency and conservation, the Energy Information Administration predicts a 45-percent increase in electricity demand by 2030 as our population and the electrification of our economy continue to increase. The electric utility industry is embarking on one of the most expansive building programs in its history with the construction of baseload generation such as nuclear and coal plants and new transmission infrastructure. Significant new coal and nuclear capacity, complemented by natural gas and renewables sources, will be needed to meet this growing electricity demand.

Congress recognized the need for a diverse energy portfolio in the Energy Policy Act of 2005. The bill provides limited, broad-based stimulus for investment in new electric power

infrastructure, including new nuclear power plants. Coupled with this growing electricity demand, the comprehensive energy legislation has stimulated companies to pursue a combined construction and operating license for new reactor designs. Nine companies, consortia or joint ventures are pursuing actions toward building between 12 and 19 new nuclear plants. These companies are developing applications for combined construction and operating licenses, which they intend to file with the NRC over the next two years. At $50 million to $90 million per application, these nine applications represent as much as $1 billion in investment by the industry in new nuclear plants. The industry also is investing approximately $500 million in the Department of Energy's Nuclear Power 2010 program.

Increasing investment by the public and private sectors in exploring the construction of new nuclear plants has generated interested on Wall Street. Fitch Ratings is one of the Wall Street firms bullish on the prospect of new nuclear plants in the near term:

> It is no longer a matter of debate whether there will be new nuclear plants in the industry's future. Now, the discussion has shifted to predictions of how many, where and when. ... New nuclear plants and baseload power plants using new coal technologies are least likely to appear in the populous and energy-hungry Northeast or in California, regions that already have significantly higher energy prices than the Southeast and Midwest. For political or geological reasons, these regions are likely to rely either on gas-fired power facilities or costly investments for other resources, such as wind or solar. These differences will tend to favor lower energy prices in the Southeast and Midwest to the disadvantage of the Northeast and California.[1]

New nuclear power plants are expected to begin operation in 2014-2015. This estimate includes approximately three years for the NRC to review the license application and four years for construction of the facility. We expect that both the application process and construction times will be streamlined as these standardized plant designs are built.

[1] "Wholesale Power Market Update," Fitch Ratings Ltd., March 13, 2006

NUCLEAR ENERGY PROVIDES CLEAN-AIR BENEFITS

NEI has testified to this subcommittee in previous years regarding the clean-air benefits of nuclear energy, including the role that nuclear energy must play in voluntary or regional agreements to reduce greenhouse gases. Without restating these benefits broadly, I would like to make a few points regarding the importance of nuclear energy for clean air and for addressing concerns about climate change.

Simply stated, nuclear power plants generate electricity without producing greenhouse gases such as carbon dioxide (CO_2). Preventing emissions of greenhouse gases with the use of nuclear power and renewable energy sources is as important as reducing the equivalent amount of emissions from electricity produced by emitting sources. For example, nuclear power plants prevented the emission of about 700 million tons of CO_2 in 2004, which is equivalent to eliminating the CO_2 emissions from all of the passenger cars in the United States.

Nuclear energy's clean-air benefits are widely recognized by policymakers and environmental organizations as they look at the issues of energy production, air quality and climate change. A February report from the Pew Center on Global Climate Change says

> [N]uclear power is one of the few options for no-carbon electricity production, [and] efforts should be made to preserve this option. However, nuclear power's ability to contribute significantly to a low-carbon future over the next 50 years depends on the ability of the nuclear industry to start expanding nuclear generating capacity in the next 10-15 years, as well as on the resolution of cost, safety, and waste storage issues.[2]

Last year, the Progressive Policy Institute (PPI), a think tank affiliated with the Democratic Leadership Council, said nuclear power is a vital energy technology that should be part of the nation's comprehensive clean-air strategy. In its report, "A New Clean Air Strategy," PPI said, "lawmakers should acknowledge nuclear power's potential not only to reduce undue reliance on natural gas, but also help combat climate change and clean up the air."

[2] "Agenda for Climate Action," Pew Center on Global Climate Change, February 2006, p. 9.

Energy ministers from the G8 countries, at a March 2006 meeting, said that joint efforts of the G8 and other countries aimed at wider use of renewable and alternative energies, development and implementation of innovative energy technologies and development of low-carbon energy would contribute substantially to fuel diversification for energy production and energy security. "For those countries that wish, wide-scale development of safe and secure nuclear energy is crucial for long-term environmentally sustainable diversification of energy supply," the ministers' statement said.

Extending the operation of today's reactors and building new nuclear power plants is imperative as part of a diverse portfolio to meet the nation's energy demand and air quality goals. Most of America's nuclear power plants were brought on line in the 1970s and 1980s. As a nuclear plant's initial operating license lasts 40 years, one-third of the 103 reactors already has applied for and received an extension from the NRC for 20 additional years. NEI expects most, if not all, of the remaining plants to apply for license renewal. If nuclear power plants are retired and not systematically replaced with new nuclear generation at the end of 60 years of operation, our nation will start losing the most important source of electricity to prevent greenhouse gas emissions.

The addition of renewable energy sources, mostly wind power, has escalated in many states, and the nuclear industry supports the role of renewable energy sources as part of a diverse energy portfolio. However, renewable energy sources cannot meet the 24/7 demand for electricity. For that reason, investment in advanced-design nuclear plants is essential to any realistic effort to significantly reduce greenhouse gas emissions.

NUCLEAR PLANTS HAVE THE BEST PRIVATE SECURITY IN THE NATION

The nuclear energy industry is committed to the most effective security at nuclear plant sites to protect the employees and plant neighbors, as well as the plants themselves. America's nuclear energy facilities must meet strict NRC regulations for security. Nuclear power plants are the

most secure commercially owned facilities in the country, and there is a high degree of public confidence that the industry can operate nuclear power plants safely and securely.[3]

The industry is proud of its security programs and the example they provide for other sectors of America's critical industrial infrastructure. I recommend that members of this subcommittee and any member of Congress visit a nuclear plant to see these security programs firsthand and meet the professionals that manage and implement our security programs. All U.S. plants meet the same high standards established and inspected by the NRC.

Compared to other commercial facilities, nuclear power plants start with a clear advantage in the area of security. The structures that house reactors and other critical systems are built to withstand natural events such as earthquakes, hurricanes, tornadoes, fires and floods. They are massive structures with thick, steel-reinforced exterior walls and internal barriers of reinforced concrete. As such, the structures provide a large measure of protection against potential attacks that were not anticipated when they were built. In addition, the "defense-in-depth" philosophy used in nuclear facility design means that plants have redundant systems to ensure safety. Many of these redundant safety systems are separated physically so that if one area of the plant is compromised, backup systems in another part of the plant can maintain safety. This redundancy provides a capability to respond to a variety of events.

Our difficult-to-penetrate structures are just the first stage of a multi-stage security strategy that also includes surveillance and monitoring, detection equipment, strict access control using biometrics and other technology, and physical security using structures and paramilitary security forces. Nuclear power plants also have concentric perimeters with increased security at each level. Physical barriers protect against vehicle intrusion, including truck bombs. These security zones are protected by trained and armed professionals, who use hardened defensive fighting positions located throughout the plant, if needed. In the innermost security zone, access to the vital areas of our plants is strictly controlled and constantly monitored.

[3] Sixty-four percent of the public gives U.S. nuclear power plants high safety ratings (5 to 7 on a 7-point scale), according to a March 2006 survey of 1,000 U.S. adults by Bisconti Research Inc./NOP World. Question: "Thinking about the nuclear power plants that are operating now, how *safe* do you regard these plants? Please think of a scale from "1" to "7," where "1" means *very unsafe* and "7" means *very safe.*"

Industry employees undergo comprehensive background checks, a systematic fitness-for-duty program and a continual behavioral observation program. Every plant also has extensive plans and arrangements to coordinate with state and local law enforcement and emergency response entities. In addition, every plant must conduct drills and exercises to ensure a well-prepared, comprehensive emergency response plan.

The combination of strong structures, perimeter protection, access controls and other security measures at nuclear power plants greatly exceeds the security provided for other elements of the critical infrastructure. The strength and safety features of nuclear power plants, including multiple safe-shutdown systems, make it unlikely that there would be a radiological release that would affect public health and safety.

The FBI considers security forces and infrastructure at nuclear power plants formidable and nuclear power plants difficult to penetrate.

The plant features that protect the public from radiological hazard in the event of a reactor incident also protect the plant's fuel and related safety systems from attempted sabotage. Redundant safety and reactor shutdown systems have been designed to withstand the impact of earthquakes, hurricanes, tornadoes and floods. Areas of the plant that house the reactor and used reactor fuel also would withstand the impact of a widebody commercial aircraft, according to peer-reviewed analyses by the Electric Power Research Institute, a Palo Alto, Calif.-based research organization.

Moreover, the Center for Strategic and International Studies (CSIS) also found that nuclear power plants would be unattractive targets to terrorist organizations because of the industry's robust security program. CSIS President John Hamre, former deputy secretary of defense under President Clinton, said that nuclear power plants "are probably our best-defended targets. There is more security around nuclear power plants than anything else we've got. ... One of the things that we have clearly found ... is that this is an industry that has taken security pretty seriously for

quite a long time, and its infrastructure, especially against these kinds of terrorist threats, is extremely good."

NRC, INDUSTRY TAKING DECISIVE STEPS AGAINST EMERGING THREATS

The NRC and the industry have undertaken decisive steps to reassess security programs and implement additional measures to ensure that nuclear plants are safe and secure, considering today's threat environment. These steps include:

- a reassessment of industry security programs and the regulations governing them
- a plant-by-plant review of security programs
- significant investment in security officers and capital improvements to strengthen plant security
- enhanced training and force-on-force exercise program
- additional programs to coordinate with federal, state and local governments to develop integrated deterrence and response capabilities
- major studies to reassess our plants' ability to withstand attack.

It is important to recognize the roles of both the NRC and the industry in securing nuclear power plants. The NRC mandates that each plant provide security to protect against the design basis threat. Although this is defined in detailed orders and regulations, it is the responsibility of electric utilities that operate U.S. reactors to define the plant-specific strategies to defend against the DBT and demonstrate that the strategies work at each nuclear plant site. It is the federal government's responsibility to determine the potential risk of terrorist attacks and to provide a coordinated approach to support the plant for attacks within the DBT and those beyond the DBT. This is accomplished using a combination of intelligence-gathering, federal law enforcement and other resources.

THE NRC AND INDUSTRY HAVE SYSTEMATICALLY IMPROVED SECURITY SINCE 2001

As NEI noted in testimony to this subcommittee in 2004, the nuclear energy industry has bolstered security at its plants, making them even more secure. Since 2001, the industry and the NRC have reviewed every facet of nuclear plant security and as a result have implemented improvements in both the regulatory requirements and the plants' physical, human and strategic capabilities.

Immediately after the Sept. 11, 2001, attacks, the NRC ordered all nuclear power plants to remain on high alert. The industry limited access to its plants, expanded protective security perimeters, constructed temporary barriers along the outer perimeter of plants and discontinued non-essential access. In addition, nuclear power plants immediately began hiring additional security personnel and upgrading overall security programs.

In February 2002, the NRC issued several interim security orders. These orders, in effect, increased the DBT with a commensurate increase in security at nuclear power plants. The industry complied fully with the NRC orders and instituted additional measures, including:

- extending and fortifying security perimeters
- increasing armed patrols within security zones
- installing new barriers to protect against vehicle intrusion
- installing additional high-tech surveillance and detection equipment
- strengthening security coordination with local, state and federal agencies to integrate approaches among these entities—a position the industry continues to support.

In the months following the NRC orders, the industry developed guidance that was approved by the agency to ensure consistent and thorough implementation of the new security requirements.

The NRC issued three additional orders in April 2003 after completing a top-to-bottom review of security and studying potential threats to nuclear power plants. The new DBT increased the size of a potential vehicle bomb and the number of terrorist attackers against which the industry

would have to defend in a ground assault. The new DBT also increased the modes of potential attack to include water-borne assaults. Each plant was ordered to make the necessary modifications to meet the new DBT by October 2004.

The NRC also issued orders that enhanced training and qualification of security officers, improved access controls at nuclear facilities and established work-hour limits for security personnel. These orders required the industry to develop and submit new security and safeguards contingency plans, as well as enhance training and qualification programs. The industry developed standardized templates to meet these new requirements and obtained NRC approval on the templates for industry use. This innovative approach assured consistent industry implementation of the security orders.

As a result of these new requirements, the number of security officers at 64 plant sites has increased from approximately 5,000 to 8,000. Other changes at every nuclear plant include physical improvements to provide additional protection against vehicle bombs and against water- and land-based assaults. Every plant has augmented security forces, increased security patrols, added security posts, lengthened vehicle standoff distances, tightened access controls, and enhanced coordination with state and local law enforcement and response organizations.

The industry has invested more than $1.2 billion in additional security measures since September 2001. Physical improvements and equipment upgrades at nuclear plants comprise the majority of this total, but the industry also has spent several hundred million dollars on additional security personnel, which represents an ongoing cost at each site. NRC security spending also has increased significantly in recent years and reached $80 million for homeland security activities in its fiscal 2006 budget.

The NRC again is reviewing the DBT for nuclear power plants, responding to concerns from various stakeholders and direction from Congress in the Energy Policy Act of 2005 to more formally adopt a new DBT in regulations. The NRC accepted public comments on its proposed rule, and the commission expects to adopt a final rule by February 2007.

GOVERNMENT ACCOUNTABILITY OFFICE REPORT ON NUCLEAR PLANT SECURITY

The GAO recently completed a report evaluating security at commercial nuclear power plants. In the process of compiling data for its assessment, the GAO met with NEI representatives and visited nuclear power plants to observe security and force-on-force drills. The industry finds the report to be well-documented, reasonably accurate and fair. While GAO identifies specific areas regarding the effectiveness of programs where improvements can and will be made, we urge members of this subcommittee and other members of Congress to consider some of the key findings of the report that relate to the more important overall programmatic aspects of security:

- "The NRC revised the DBT for nuclear power plants using a generally logical and well-defined process in which trained threat assessment staff made recommendations for changes based on an analysis of demonstrated terrorist capabilities. The process resulted in a DBT requiring plants to defend against a larger terrorist threat, including a larger number of attackers, a refined and expanded list of weapons, and an increase in the maximum size of a vehicle bomb."

- The industry "made substantial security improvements after the Sept. 11, 2001, attacks and in response to the revised DBT. At the sites we visited, these actions included, for example adding security barriers and detection equipment, implementing new protective strategies, enhancing access control and hiring additional security officers ... The site's efforts have been substantial and, in some cases, have gone beyond what was required."

- "NRC has taken a number of actions as part of its restructuring of the force-on-force program that satisfy the recommendations we made to strengthen the program. ... the attackers in the force-on-force exercise scenarios we observed used many of the adversary characteristics of the revised DBT ... In addition, NRC officials told us that the adversaries were trained in military tactics."

Appropriately, NEI and its member companies have been engaged with the NRC in taking these significant steps to improve security at nuclear power plants. At the request of the NRC, the

industry has provided comments on specific aspects of its evolving requirements. The NRC has agreed with some of our recommendations, but certainly not all of them. We believe that the NRC acted appropriately in seeking and considering the views of government entities as well as the industry prior to making changes to its security requirements.

As noted by the GAO, however, the NRC followed an unusual process of seeking input while simultaneously analyzing intelligence information. This is hardly surprising considering the heightened national concern over homeland security. In addition, the NRC cannot publicly disclose safeguarded information regarding nuclear plant security, making an open debate over those details difficult, if not impossible.

Even with the NRC's set of new requirements and significant measures taken by the industry to enhance security, making these facilities secure from potential threats does not end with the industry's comprehensive measures. It is vital that industry security be integrated with local, state and federal resources. Some postulated threats, such as attacks by large forces or by forces using advanced weaponry, are beyond the industry's DBT and are the responsibility of the federal government and the military. Privately funded security forces have practical and legal limits on the force they can use and, thus on their overall capabilities to defend against an attack.

The GAO recognized this point when it stated that "consideration of issues such as what is reasonable to defend against is an appropriate role of the commission in approving changes to the DBT." The DBT is a requirement placed upon the companies that operate nuclear power plants and cannot be greater than what licensees reasonably can be expected to provide. That does not mean, however, that the DBT represents the outer limits of security that is provided at our plants.

The nuclear energy industry recognizes that there is a theoretical possibility of an attack beyond the capabilities of plant security. In such cases, plant personnel would help respond in coordination with local, state and federal authorities. The industry has provided national leadership in this area by being one of the first industrial sectors to establish a Sector

Coordinating Committee with DHS to provide a forum for integrating industry and off-site resources for threats that exceed our stand-alone capabilities.

In addition, the nuclear energy industry is the first industrial sector to participate in the DHS Comprehensive Review Program. The comprehensive reviews examine every element of the critical infrastructure, including a thorough security assessment, and DHS provides recommendations on additional measures that can be taken to protect against and mitigate possible terrorist attacks. The assessment and recommendations involve local, state and federal authorities with the goal of achieving the most effective allocation of resources across the various sectors of the critical infrastructure.

During these comprehensive reviews, a multidisciplinary team spends a week reviewing a site's vulnerabilities and security plans and also spends three to five days at the site interacting with security personnel, emergency planning and response staff, and state and local law enforcement and emergency responders. More than 20 nuclear plant sites already have participated in this program, and we expect that all nuclear power plants will complete comprehensive reviews by July 2007.

The nuclear industry also has completed 22 assessments using the Department of Homeland Security's Risk Assessment and Management for Critical Asset Protection (RAMCAP) model. This program provides comprehensive vulnerability and consequence assessment and is a tool that is used for informing the agency's comprehensive reviews.

Clearly, the industry is fully committed to working with all levels of government to provide the best security possible to deter an attack and to respond forcefully and swiftly should one occur. The industry must always satisfy the security requirements imposed by the NRC, yet it is constantly working to improve security at nuclear plants through training, drills and exercises; implementation of new technology; and cooperation with government entities such as DHS, FBI and local law enforcement.

FORCE-ON-FORCE EXERCISES HAVE BEEN IMPROVED SIGNIFICANTLY

The industry is pleased that the GAO has recognized the many improvements that have been made to the force-on-force security exercises that are used uniquely by the nuclear industry to test, as realistically as possible, our security programs and systems. Most of the GAO's recommendations for industry in this area already have been implemented.

The GAO is incorrect, in a sense, when it says that the revised DBT has been tested at only about a third of our sites. The DBT has been tested at all nuclear plant sites and the NRC has evaluated half of them. The NRC evaluates force-on-force exercises every three years at every site and is following an aggressive schedule of overseeing more than 20 exercises per year.

The industry also conducts multiple other force-on-force drills annually that are not supervised by the NRC. These exercises are part of the ongoing programmatic training and drilling cycle for our security officers. These additional drills and exercises allow the industry to continually test our protective strategies. These quarterly drills and annual exercises are comparable to the full-scale, force-on-force drill observed every three years by the NRC.

POLICY IMPLICATIONS OF INCREASING NUCLEAR PLANT SECURITY REQUIREMENTS

The industry recommends that Congress and other policymakers bear in mind that security at our nuclear power plants is a shared responsibility between the plant owners, the NRC, federal, state and local government. The industry has made significant investments in its security programs, which are unparalleled in the industrial sector, and we are committed to providing the necessary security at our sites. In this regard, the industry believes the greatest enhancement in security around nuclear plant sites will now occur when we develop comprehensive strategies that combine our security and emergency response resources with those of local, state and federal entities to fully protect these facilities and the people who work and live near them against the threats deemed appropriate by the federal government.

The industry has recognized the need to develop coordinated response capabilities to prevent and respond to potential attacks on our critical infrastructure. Through our activities with the NRC, DHS and other government entities, the nuclear energy industry has been a leader in these efforts, and we encourage members of this subcommittee to remain engaged on this issue to ensure that every sector in the critical infrastructure follows suit. The nuclear energy industry is justifiably and understandably proud of its leadership and accomplishments in the area of security. We are pleased that the GAO agrees that our security has been improved greatly, and we will continue to work with government agencies and Congress to address emerging issues.

Security at America's nuclear facilities was exceptional prior to Sept. 11 and is even better today. It is highly unlikely that attackers could successfully breach security at a nuclear power plant, and even more unlikely that they could achieve a result that would endanger the residents near our facilities. Yet, security at our nuclear power plants is not static. We constantly are assessing and testing our security programs. Consequently, America's nuclear energy industry will remain a leader and model for protecting our nation's critical infrastructure.

Mr. SHAYS. Thank you, Mr. Fertel.
Mr. Crane. Thank you.

STATEMENT OF CHRISTOPHER CRANE

Mr. CRANE. Chairman Shays and subcommittee members, I am Chris Crane, president and chief nuclear officer of Exelon Nuclear, and I am pleased to be here today to continue on with what Mr. Fertel provided as to what the industry has done, but give you more specifically what's happened in our company, Exelon.

Exelon Generation is the largest owner and operator of commercial nuclear power plants in the United States. We own and operate 17 reactors in 10 States—Illinois, New Jersey, Pennsylvania. In addition, we provide the management and operating assistance for three reactors in New Jersey that are owned by Public Service Enterprise Group [PSEG].

Exelon is extremely proud of our operating performance. Our plants are among the best in the world in terms of capacity factor and outage management. We are even more proud, however, of our safety record. Our highest duty is to protect the safety and security of our workers and the people who live within the communities around the plants that we operate.

As a result of the NRC revised security requirements, Exelon Nuclear invested $140 million capital improvements for the physical security upgrades at our plants. In addition, we have greatly increased the staffing of our security forces, but the contracts——

Mr. SHAYS. Mr. Crane, I am going to just interrupt you for a quick second.

I have to go before the Rules Committee. We are going to keep going. I am going to have Mr. Duncan chair, and I am going to ask Mr. Van Hollen, if he doesn't mind, to chair if Mr. Duncan has to leave. And then I will come back.

Then, if you would, if you would have counsel ask some questions as well? And I hope I will be able to get back in time to ask the questions I want.

Sorry to interrupt, but I just wanted to make clear what we are doing.

Mr. CRANE. As I was saying, we, as a company, have invested over $140 million in capital improvements and our physical security upgrades at the sites. In addition, we have greatly our staffing of our security forces, with our contract forces expanding by 84 percent and our corporate security organization, which provides the oversight and strategic development and coordination of our security plans, increasing by 20 percent.

In 2001, our security-related operating costs were approximately $44 million. This year, we expect to spend $90 million for security.

All Exelonsites have complied with the NRC requirements regarding infrastructure improvements, training requirements, and access authorization. As part of the NRC's effort to confirm continued compliance with these security standards, the Commission conducts routine inspections that have been discussed here today.

This year alone, we have conducted multiple exercises at all the facilities. We conducted multiple sites at all of our facilities. We have had two force-on-force drills that were discussed about pre-

viously last year, and by the middle of this year, we'll have two additional that will be completed.

While security at the commercial nuclear plants in the United States has improved greatly since 2001, performance issues can and do arise with security personnel. As these issues arise, they are addressed systematically and objectively.

As I noted earlier, Exelon assumed the responsibility last year of the management of the PSEG's Salem and Hope Creek reactors. The shift came in an aftermath of an inadequate force-on-force exercise at the Hope Creek project or the Hope Creek site, which was referenced earlier in the GAO report and has been referenced by different panelists here today.

As our first order of business, we installed the Exelon defensive strategy model at the site, investing approximately $40 million that's above and beyond the $140 million we've previously spent in capital improvements. We also increased the security force by approximately 40 percent in 2005. And as a result of these efforts, Salem and Hope Creek successfully passed the evaluated exercise, and we consider that a great success.

As a part of the Energy Policy Act of 2005, Congress directed the NRC to conduct formal rulemaking to review its design basis for the commercial nuclear facilities. Clearly, the Commission, as stated previously, must continue to assess the threat facing the nuclear plants for possible changes.

In conducting this assessment, we recommend that the Commission should continue to closely coordinate with the Department of Homeland Security and Federal intelligence and law enforcement agencies. In addition, the Commission, in evaluating these potential changes to design basis threat, must keep in mind the different delineations between the responsibility of the plant owners, those of law enforcement, and for the Federal Government.

While Federal law requires plant owners to protect against various potential threats, the law also considers many threats to be outside the scope of the licensee's responsibility and instead relies on law enforcement and the military to protect against these certain threats.

Mr. Chairman, Exelon is committed to safe operations of our plants and providing strong security and emergency planning programs. We have devoted significant financial and personnel resources to ensure that our sites are in full compliance with the NRC requirements.

We have established high performance expectations for our security forces. We continue to work closely with the NRC and Federal, State, local enforcement to ensure that we have fully integrated a plan to respond to security events at our site.

I'd like to thank you again for the opportunity to provide this input and would welcome any questions you may have.

[The prepared statement of Mr. Crane follows:]

Statement of

Christopher Crane
President and Chief Nuclear Officer
Exelon Generation

Before the National Security, Emerging Threats
And International Relations Subcommittee

Committee on Government Reform
U.S. House of Representatives

April 4, 2006

Mr. Chairman, I am Chris Crane, President and Chief Nuclear Officer of Exelon Generation. Thank you for the opportunity to appear before you today to discuss the safety and security of the nation's commercial nuclear power plants. While my colleague Mr. Fertel from the Nuclear Energy Institute has provided the panel with a broad industry perspective, I would like to provide you with a summary of Exelon's experience in strengthening plant security.

Exelon Generation is the largest owner and operator of commercial nuclear power plants in the United States. We own and operate 17 reactors at 10 sites in Illinois, New Jersey, and Pennsylvania. In addition, we operate three reactors in New Jersey that are owned by Public Service Enterprise Group (PSEG). Exelon Nuclear employs over 7,000 people, many of whom live within the 10 mile emergency planning zones around our plants. We also employ thousands of contractors, including over 1,200 security personnel at our 10 sites.

Exelon is extremely proud of our operating performance, and our plants are among the best in the world in terms of capacity factor and outage management. We are even prouder, however, of our safety record. Our highest duty is to protect the safety and security of our workers and of the people who live and work in the communities in which we operate.

Background on Nuclear Plant Security

At the time of the terrorist attacks on our nation in 2001, nuclear plants were already the most secure industrial facilities in the United States. Since the inception of the nuclear era, commercial nuclear plants have relied on a defense in depth strategy to protect the public from radiological risk, beginning with the design and construction of the reactor. Nuclear plants include multiple layers of robust physical protection and redundant safety systems to protect against a release of radiological material.

At Exelon, we were spending roughly $44 million per year on security prior to 9/11. Like other plants, Exelon had a comprehensive security plan for each of our sites that included a complete assessment of potential threats and vulnerabilities, extensive barriers to protect against intrusion, high-tech surveillance equipment to monitor the site, and a well-trained security force. In addition, the industry had a well-established program to screen potential and current employees, including criminal background checks that were conducted by the Federal Bureau of Investigation. These programs were integrated with state and local law enforcement and were reviewed and approved by the Nuclear Regulatory Commission.

In response to the terrorist attacks and subsequent NRC directives, security at Exelon facilities was elevated to its highest level. As part of our response, we extended the point of initial screening of people entering the plant site form the protected-area boundary (that immediate area around the physical plant) to the owner-controlled area boundary (the area encompassing the entire site property). State police and, in some cases, National Guard personnel, augmented that initial identification and inspection of people entering the site. In addition, armed security forces extended their patrols to include the owner-controlled area boundary.

Exelon and other reactor operators took a variety of additional protective measures in conjunction with NRC guidance, including additional background checks for certain

plant personnel, additional screening and control of all on-site deliveries upon entry to the owner-controlled area, an increased number of security officers and armament, and increased senior management presence and visibility.

During the immediate aftermath of the terrorist attacks, the nuclear industry worked closely with a variety of Federal, state and local officials to identify additional safeguards and resources to assure the continued security of nuclear plants. Among the Federal agencies consulted were the Nuclear Regulatory Commission, the Office of Homeland Security, the Federal Emergency Management Agency, the Department of Energy , the Department of Defense, the Federal Bureau of Investigation and the National Infrastructure Protection Center.

It is worth noting that, at this time of national crisis, other industries turned to the nuclear industry as a model for providing security at commercial facilities. Nuclear plants were, and continue to be, viewed as the most well-protected industrial facilities in the United States.

NRC Actions to Strengthen Plant Security

As noted above, the NRC took immediate action on September 11, 2001, to elevate security at commercial nuclear power plants to their highest level. On February 25, 2002, the Commission issued a series of interim compensatory measures which imposed significant additional requirements on plant operators pending the completion of a more comprehensive review of safeguards and security program requirements. These requirements addressed security officer staffing levels, protection against potential vehicle and waterborne threats, protection of used nuclear fuel stored at reactor sites, enhanced access authorization controls, and mitigation efforts in the event of an attack.

In April 2003, the Commission issued a set of security-related orders which revised the Design Basis Threat (DBT) – the threat against which plant operators must defend,

established training and weaponry requirements, and enhanced access authorization requirements. These orders resulted in significant security enhancements, both in terms of physical infrastructure improvements and additional human resources.

As a result of the Commission's revised security requirements, Exelon Nuclear has invested over $140 million in capital improvements for physical security upgrades at our plant sites. These upgrades have included the installation of military-grade protective fencing, vehicle barriers, surveillance equipment, and guard towers at each of our sites.

In addition, we have greatly increased staffing for our security forces, with our contract security force expanding by 84 percent and our corporate security organization, which provides management oversight, strategy development and coordination, increasing by 20 percent. In 2001, our security-related operating costs were approximately $44 million annually. This year, we expect to spend $90 million for security.

Prior to 9/11, nuclear plants worked closely with state and local law enforcement and the Federal Bureau of Investigation to coordinate both emergency planning and security. Exelon has expanded our coordination with external response agencies, including the Department of Homeland Security, and these agencies have reaffirmed their commitment to provide additional resources in the event of an attack at reactor sites. We continue to work with law enforcement agencies to ensure an effective and fully integrated response to any security event at our sites.

Given the progress made to date on improving security infrastructure and personnel at reactor sites, the integration of Federal, state and local resources to support the already significant security capability at plant sites is perhaps the most important thing the government can do to enhance security further.

All Exelon sites have complied with the NRC's requirements regarding infrastructure improvements, training requirements and access authorization improvements. As part of the NRC's effort to confirm continued compliance with these security standards, the

Commission conducts routine security inspections and exercises at plant sites. This year alone, the NRC has conducted security-related inspections at seven of Exelon's 10 plant sites and has conducted baseline inspections at three sites. In addition, the NRC has conducted force-on-force exercises at two Exelon sites since last August, and force-on-force exercises are scheduled to occur in the next two months at two other Exelon sites.

While security at commercial nuclear plants in the United States has improved greatly since 2001, performance issues can and do arise among security personnel. As these issues arise, they are addressed systematically and objectively. As I noted earlier, Exelon assumed responsibility last year for the management of PSEG's Salem and Hope Creek reactors. We began to manage these plants in the aftermath of an inadequate force-on-force exercise at the Salem/Hope Creek site. As a first order of business, we installed the Exelon defensive strategy model at the site and invested approximately $40 million in capital improvements in 2005 alone. We also increased the security workforce at the site by approximately 40 percent during 2005. As a result of our efforts, Salem/Hope Creek successfully passed an evaluated security exercise.

Looking Ahead: Further Improvements to Plant Security

As part of the Energy Policy Act of 2005, Congress directed the NRC to conduct a formal rulemaking to review its Design Basis Threat for commercial nuclear facilities. The current DBT was established by Commission order. Congress also provided the Commission with guidance in terms of specific issues that must be considered during that rulemaking. The Commission has begun the public comment period on the proposed rulemaking and is expected to issue a final rule no later than February 2007.

Clearly, the Commission must continue to assess the threat environment facing nuclear plants for possible changes. In conducting this assessment, the Commission should continue to consult closely with the Department of Homeland Security and Federal intelligence and law enforcement agencies. In addition, the Commission, in evaluating potential changes to the Design Basis Threat, must keep in mind the current delineation

between the responsibilities of plant owners and those of law enforcement and the Federal government. While Federal law requires plant owners to protect against a variety of potential threats, the law also considers many threats to be outside the scope of licensee responsibility and instead relies on law enforcement agencies and the military to protect against certain threats.

Conclusion

Exelon is committed to the safe operation of our plants and to providing strong security and emergency planning programs at each site. We have devoted significant financial and personnel resources to assuring that our sites comply fully with all NRC requirements, and we have established high performance expectations for our security forces. We continue to work closely with the NRC and with Federal, state, and local law enforcement to ensure that we have a fully integrated plan to respond to security events at our sites.

Mr. Chairman, thank you again for the opportunity to appear before you today. I look forward to answering any questions that you and the members of the subcommittee may have.

Mr. DUNCAN [presiding]. Well, thank you very much, Mr. Crane. You have certainly been an informative panel.

I will say something that I have told other people at times. Chris Shays is not my Congressman either, Ms. Brian, but I will tell you that—and Mr. Blumenthal, if he doesn't already know this, should know this—that Chris Shays is one of the most active and one of the finest chairmen that we have in this Congress today.

I don't always agree with him, and he would be very proud to tell you that I don't always agree with him probably. But at any rate, he does an outstanding job, and this hearing is another example of that.

I told him I have a whole host of appointments starting at 3:45, which was 5 minutes ago. So I am not really going to ask any questions except for this.

What percentage of our energy now is generated by nuclear power? I am sure Mr. Crane or Mr. Fertel can tell me.

Mr. CRANE. Greater than 20 percent.

Mr. DUNCAN. Well, and what I am getting at, I had read something similar to that, and I have also read, though, that some other countries like France and Japan and Sweden and some others, they have—I believe I read that some country has as high as 70 percent.

Can you tell me anything about that? What percentage some of those other countries?

Mr. FERTEL. I think France is up around 70 percent, Congressman Duncan, and I think one of the former East Bloc countries actually is close to 80 percent.

Mr. DUNCAN. Oh, really?

Mr. FERTEL. Yes. I think 20 percent in our country, we'd like to see more. But to be honest, it's still the largest program in the world. The nuclear program in this country is bigger than the French and Japanese programs combined, and they're the second and third largest programs.

So in number of plants and output, we are actually very large. In percent of our total electricity supply, we're still the second largest, but only 20 percent.

Mr. DUNCAN. Well, I was a lawyer and a judge before I came to Congress, and I am not a nuclear expert by any means. And I will say this. I have always said and believe that anybody can improve.

I hope I am a better Congressman now than I was 5 years ago. This is my 18th year. I hope I am better now than I was 5 years ago. And if I am here 5 years from now, I hope I am better then than I am now.

And we should all strive to get better, and I hope that the nuclear industry takes very seriously, and I believe they will, the recommendations or suggestions of the GAO.

On the other hand, I do know from reading that the nuclear industry in this country is one of our most highly regulated industries, even at this point, and that this industry is probably more highly regulated in this country than in any other country. And saying that, I will make it very clear to tell everyone that I have no connection whatsoever, even remote, to the nuclear power industry.

So, you know, my father told me many years ago about something else. I don't even remember what he was talking about. He

said everything looks easy from a distance. And it is real easy to criticize, I can assure you, on almost anything.

But you know, I know, too, common sense would tell you that the nuclear industry would be the most concerned about a terrorist attack because you are talking about losing whopping amounts of money if they had a plant that was attacked and closed down.

Now I heard a speech by Secretary Chertoff a few months ago in which he said it is not possible to protect against every conceivable harm at every place at every moment. So, what we have to do, we have to do what is reasonable, what is practical, yet we can't sacrifice the good to try to achieve the perfect. I mean we could shut the whole country down, and we wouldn't have any nuclear concerns or any other, you know, but that makes no sense whatsoever.

So I think the nuclear power industry, frankly, is doing a great job. I am sure that there probably were people at the NRC who were offended to hear that the nuclear power industry had too much influence over them because they say that their report is based on contributions from Federal, State, and local officials, all kinds of stakeholders, and everybody who has really much of an interest at all.

But I am going to go to those appointments, and I am going to turn this over to Congressman Van Hollen for any questions he has. And then I understand the staff is going to ask some questions.

Thank you for taking over.

Mr. VAN HOLLEN [presiding]. Well, thank you. Thank you, Mr. Duncan. And let me also thank our witnesses.

Unfortunately, I, too, have a group waiting back in my office. I apologize. I missed the first panel because the Government Reform Committee, another subcommittee had a hearing as well.

I just have two questions. The first question is for Mr. Fertel and Mr. Crane. With respect to the analysis of the vulnerability of nuclear power plants to an air attack, we know from investigations by the 9/11 Commission and others that was one of the scenarios envisioned by the September 11th attackers.

Putting aside the question of who is responsible for dealing with that issue, would you agree that is a vulnerability in the system that needs to be addressed, or is that something that is, in your view, such a low probability we shouldn't worry about it?

Because as of right now, we haven't done much about that as a Nation. We have sort of been pointing fingers as to who is responsible for addressing the issue rather than tackling the issue.

Mr. FERTEL. Just a response to that. First of all, from a pure technical study standpoint, the NRC has done studies, and I'm sure they can brief you in their secret session.

The industry did studies that we don't hold secret. We hired the Electric Power Research Institute shortly after September 11th to look at a 767–400, a relatively large plane, one that constitutes more than 80 percent of the aircrafts flying in this country and had it hit containment structures where the fuel is, had it hit spent fuel pool structures, and had it hit dry cask storage.

And they did it as an analysis to maximize the impact, and what we found was we wouldn't get a release of radiation with that particular scenario.

Now National Academy of Sciences looked at things and said, well, if the plane was bigger, and the plane flew faster, you get a different outcome, no question. The plane doesn't hit it just right, you get a different outcome.

So what we concluded was that the robustness of the structure is really pretty good unless you have a really marvelous hit on the structure. A very, very bad day at the plant with a lot of people dead that work there, but as far as a release, we didn't get it from a relatively sophisticated analysis. This was $1 million worth of engineering computer runs.

You weren't here for the first panel, Congressman, but Commissioner McGaffigan and others talked about the actions they have taken. They've taken actions with NORAD and with the military to do a number of things as far as trying to protect the air space around nuclear plants, imminent threat procedures at all of Mr. Crane's plants.

His control room has been trained on basically shutting the plant down if they're told by NORAD something happens or a plane is off course. They don't have to know it's a terrorist plane. They've also been trained on other actions they could take to try and put the plant in the safest condition it could be in if there was something that happened.

So there have been a lot of actions taken by the Nuclear Regulatory Commission. Studies are still being completed right now looking at things like that at the plants. What's not being done is what you said, which is, you know, putting surface-to-air missiles at every plant.

And we would say that things like that come out of these comprehensive reviews that I mentioned. The comments made by Danielle and the attorney general say that there are threats bigger than the DBT. We don't question that. Of course, there are. There's threats smaller than the DBT, too.

But there are bigger ones, and what the Department of Homeland Security is doing is looking at a spectrum of 16 threats, many of them larger than ours, much larger, and many of them smaller. And they are looking at airplanes and figuring out what they should be doing for particular sites.

Mr. VAN HOLLEN. Thank you.

Does anyone else have a comment on that question?

Mr. BLUMENTHAL. Only, Congressman, that if I understood the response correctly, it was that, yes, we should be looking at the potential for aircraft attack, despite a study or a number of studies that perhaps show that it can be exaggerated. But clearly, it is a threat in places like Millstone or Indian Point, given the vulnerability of the structures there.

And I think maybe equally important, and certainly the non-engineers, the citizens among us will appreciate this point, this fear is a very real one for people who live near the plants. And that includes people who live within a 50-mile radius, which is the zone that's regarded at risk, which includes a third of the population of

Connecticut, when it comes to Indian Point and even larger if you consider Millstone.

Mr. VAN HOLLEN. Right. No, thank you on that point.

I think that you are right. This is clearly an area that we need to move forward on more aggressively. There is no doubt about that. Both in terms of the physical protection of the plant areas, but more important in terms of the interception.

Let me just ask, if I could, Ms. Brian, most of the testimony today is focused on nuclear power plants. There was this investigation that was done last fall with respect to nuclear research reactors at different universities around the country and the ability of people to get easy access to those research facilities.

And after that, there was discussion about, you know, how we need to tighten up on security. And I don't know if you have had an opportunity, or if any of the other members of the panel, but if you have had an opportunity to look at what has been done, whether it is adequate, and if not, what more we should be doing?

Ms. BRIAN. Yes. Well, I am familiar with that. That was an ABC investigation.

And the one thing that was a little confused by that investigation was not all research reactors really are the same. Many of them have such small amounts of nuclear material that they're not of great consequence.

There are some, however, though, that are of greater consequence than the power reactors that we're talking about here. It's actually weapons-grade highly enriched uranium. And while one reactor doesn't have enough to make a bomb, two would.

And one of the things that we've been talking about—in fact, we're going to be testifying tomorrow before Armed Services on the subject—is that those reactors—I'm sorry—those facilities are regulated by the NRC. And while they do have a higher standard of security than they do for the power plants, it's not as high as the standards of the Department of Energy for exactly the same materials.

And I think it's one of these weird bureaucratic, "Well, it's another agency, even though it's the same material" kind of thinking. And we're in the process of working with the Department of Energy to rethink shouldn't they be taking over responsibility and dramatically increasing standards?

There is also a real question, why do the universities need to have HEU at all?

Mr. VAN HOLLEN. Right. I understand that the GAO is taking a look at security at the research reactors as well, and we are looking forward to their report on that. My understanding is research reactors, yes, you have some with more highly enriched uranium, which is actually potential bombmaking material. But even those that are less highly enriched have the potential for use in some kind of dirty bomb with a conventional explosive.

So I mean, to your knowledge, and I must I happened to be channel surfing, I think—and I saw some of the expose on that. And people were just able to walk right up and get access to these plants. Has action been taken, to your knowledge, to better protect those areas and bring it up to some of the standards?

You say that we don't meet the same standards as the DOE does. What actions have been taken with respect to those university sites since that report?

Ms. BRIAN. To my understanding, the Government hasn't changed any of its standards at all. That's something that each university is dealing with. But I think it's very appropriate for the Government to set higher standards.

Mr. FERTEL. I can't attest to exactly what NRC as to research reactors is doing, Congressman. But submit questions to them because they have taken actions to increase security at not only commercial nuclear plants, but at research reactors and at other facilities that they regulate.

Mr. VAN HOLLEN. Good. Well, we will do that. And again, thank you all for your testimony here this afternoon. And I apologize as well.

If we could just recess until 4:15, I guess Congressman Shays will be back.

Thank you all.

[Recess.]

Mr. SHAYS [presiding]. In my 12 years as chairing a subcommittee, I have never adjourned it, and I apologize for having that happen. There is always a first.

I will just catch my breath and have counsel ask some questions, and then I want to jump in.

Mr. HALLORAN. Thank you.

Let us talk about the issue raised by the attorney general in terms of the security of spent fuel pools. Why isn't that a more explicit element of the DBT in your view?

Mr. BLUMENTHAL. I'm sorry. Could you——

Mr. HALLORAN. Sure. You raised the issue of security of spent fuel pools and their limited protection structures and other vulnerabilities. And it doesn't seem to be an explicit aspect of the DBT now. And I am wondering, in your experience, why that is, and what might be done to mitigate that risk?

Mr. BLUMENTHAL. You know, I have to apologize that I don't know the reason why it is not included in the DBT. It may well be that, and I think this response may be anticipated from others on the panel, that it is regarded as a problem that was supposed to be solved through another means. That is through transfer of that spent fuel to other locations, more secure locations. In fact, locations where the security was anticipated to be like night and day compared to what exists now.

The present facilities are temporary, putting "temporary" in several layers of quotes. But they are, nonetheless, for the foreseeable future likely to be there. And I think also there are probably technical reasons that perhaps the engineers have minimized the dangers.

But the fact of the matter is that breaching the security and creating an environment that will permit a release of radioactive material is a real danger, and there's been virtually no attention to it, at least so far as the design basis threat is concerned.

Ms. BRIAN. Mr. Halloran, if I could add, the spent fuel pools are actually a part of the DBT. Our understanding is they are one of the targets.

The concern that we share with the attorney general, though, is that there isn't enough attention placed on the kinds of things that could happen like the kinds of weapons that could be used against them, as well as aircraft, and the consequences of those, which were very well discussed in the previously mentioned National Academy study.

Mr. CRANE. OK. Again, to reaffirm that last statement. The spent fuel pools are targets that are protected by the weaponry in the DBT.

So they're drilled on. They're tried to get access to during the adversary forces. They're a part of it. What is not part of it, which is not part of the DBT—it's beyond the capability, as previously said—to protect against the airliner.

Now the NRC has taken actions, and we've all complied with the actions, and this is the confusing point. It is the actions have not been taken under the DBT. They've been taken under safety guidelines and regulations that have been issued.

We have to do certain things with our spent fuel. We have to move it in a certain location. We have to have or are heading toward having capacities for different coolant sources being added. I want to make sure I don't get into safeguards information. But there is a significant amount of work that's being done.

We would like to have the repository open to further move the amounts of used fuel. But right now they are safely and adequately stored. There are actions that the industry has taken at the direction of the NRC to have further defense and depth in contingencies available. But I think we're confusing what the DBT is and what the DBT isn't and how we protect the spent fuel pools.

Mr. SHAYS. I don't understand what you just said. What are we confusing?

Mr. CRANE. Asking why the spent fuel pools are not protected under the DBT.

Mr. SHAYS. But explain your comment, "we're confusing." What are we confusing?

Mr. CRANE. The guidelines that the NRC has issued that takes the defense and depth actions on the spent fuel pools were issued as guidelines under safety aspects, not under security.

Mr. SHAYS. And but your testimony would also be that it is part of the DBT?

Mr. CRANE. As the DBT, we protect the spent fuel pools against the armament and the forces that are prescribed in the DBT.

Mr. SHAYS. Right. Not what?

Mr. CRANE. The airplane.

Mr. SHAYS. Right. That is because we have said that is part of the Federal Government's responsibility?

Mr. CRANE. That's correct.

Mr. FERTEL. Maybe just to add a little more. Commissioner McGaffigan is sitting here, and maybe he can figure out how some of what they do that isn't safeguards so they can get out more because he's very good about doing that. But the NRC is doing and actually has completed independent assessments of every plant's spent fuel pool, looking at what could happen under very bad days.

In parallel, but also independently, the industry did its own assessment of those. Danielle referred to the National Academy

study. The National Academy study, which is a classified document, does recommend two particular remedial things you should do to deal with a bad day with spent fuel pools.

Mr. HALLORAN. Excuse me. Those studies were done under the safety rubric, though, not the security side of the house. Is that what I would understand?

Mr. FERTEL. They were done as part of requirements that the NRC imposed to look at what would happen to the spent fuel pool under airplane attacks and other things like that. It was not specific to a threat.

The actions the NRC has taken have looked at improving safety in those situations. And basically, the NRC has taken actions in one case that satisfies one of the two NAS recommendations, and the industry has proposed action that would satisfy the second case. And we think NRC is reviewing that to see if they'll approve it.

So, to be honest, the spent fuel pools are a target set as part of what you look at to protect. So while they're not "in the DBT," the DBT is applied to them, and you've got to protect them successfully against it. And second, for things that's beyond the DBT, that's been looked at very aggressively by the NRC in site-specific independent studies. And every plant is taking action to improve the safety of the spent fuel pool.

Mr. HALLORAN. That leads then to the question about enemy of the United States and of what real relevance or practical meaning that standard would have if, as was testified earlier, it was a standard crafted with a particular situation in mind. Maybe it was from Cuba.

In the terms of designing the DBT, what does it really mean when we are dealing with threats crafted by non-state actors, trans-national characteristics, they are not supported by the power of the state? One guy training to fly an airplane did a lot of damage, several guys. And so, of what real relevance is that standard today?

Mr. BLUMENTHAL. If I can take a crack at the answer first? That's the problem with the distinction, that it has little, if any, relevance today. Maybe it did in the cold war setting, where the major threat was a missile or an airplane coming from the Soviet Union and threatening a designated target. But today, an enemy of the state is not coming from outside our borders necessarily, but inside.

And the distinction, as I indicated earlier, I think is decreasingly relevant, if it has any meaning at all today. And I think the kind of distinctions which I have to admit, I didn't follow the last answer—to say that it's not in the DBT, but it is covered by the DBT. I think that kind of—and I don't question the veracity, the truthfulness of it. But I think that kind of distinction indicates the lack of relevance that this kind of attempt to use outmoded concepts has in this new world that we've occupied for the last 5 years.

Ms. BRIAN. If I could just make two points? One is if you think about an attack happening, how is a security officer supposed to figure out whether they're an enemy of the state or not? When are they going to say, "This isn't my problem?"

I mean it's so impractical in the extraordinary fast timeframe this is all happening, the chaos. It's a ridiculous concept to me. And then, in reality, the——

Mr. SHAYS. Ms. Brian, I am not fully following. Be more specific. What is a ridiculous concept?

Ms. BRIAN. The idea that the security officers are required to make a distinction between they are to protect against certain types of actors, but not others. How are they supposed to figure out whether the person who's coming in with a gun is an enemy of the state or not?

Mr. SHAYS. No, see, I happen to agree with a lot of your positions, but I think that is stretching it a bit. And if I am wrong, then you can correct me.

But, and I do agree with Mr. Blumenthal about the relevancy. But if, in fact, we are not going to say to the operators of a plant that they have to defend against an airplane coming in.

But it does raise the point, maybe you would, unless we decide, for instance, with spent fuel, which I happen to agree with Attorney Blumenthal that spent fuel is a huge risk outside the dome, outside the protective cover—I would then say, well, you know, it is the responsibility of the operators to protect it better.

So I guess I am kind of in between here, and I may even ask the Commissioner to step back and help me, walk me through this. So, which by the way, I appreciate that you would stay and listen to this other panel. It speaks well.

I think we had some folks from GAO and others who stayed, and that is appreciated as well.

Ms. BRIAN. If I could clarify my point? The aircraft is not the only thing that is eliminated from what the private security forces are required to protect because of this standard.

Mr. SHAYS. Give me an example that you would think——

Ms. BRIAN. The other weapons that we're concerned about that are not being included are considered weapons that are used by enemies of the state.

Mr. SHAYS. Maybe Mr. Fertel or Mr. Crane, you could——

Mr. FERTEL. Let me, first of all, Danielle—and I think you don't mean it the way I'm hearing it, too. The officers are not either counting the number of people attacking or asking what their weapons are to see whether they're going to fight them. They're going to fight them if they attack the site with whatever they come with.

So I don't think there is a distinction that they're not going to fight me because they think I'm an enemy of the state, but they will fight you because they think you're not.

I personally would agree, this is personal, that the enemy of the state is probably an artifact of a different era. But for the same reason, I think that you need to think about what we've been discussing differently, too. Since September 11th, this Nation has done a lot, including standing up DHS—and whether it's standing on both legs very firmly is probably in the eye of the beholder—creating a director of national intelligence, and doing a lot to try and protect our Nation.

Before that happened, NRC was kind of alone doing what it does, and I think that they have done a very good job since September 11th in making a lot of changes——

Mr. SHAYS. I don't know if you are answering the question, though, that we were discussing?

Mr. FERTEL. Well, the question was do we believe there's a distinction between enemy of the state or not, and that's what I'm addressing. Do I have the question right, Mr. Chairman?

Mr. SHAYS. Yes, but I am thinking particularly of should it be the responsibility of the operators to provide a hardened target for spent fuel?

Mr. FERTEL. Yes, OK. I didn't think we were focused only on spent fuel, but if we want to start with spent fuel. We have a hardened target for spent fuel.

Mr. SHAYS. No, but—well, you do and you don't.

Mr. FERTEL. No, we do. And I'd love to be able to have the NRC or us brief you on that, OK? They are not sitting out there by themselves. You weren't here, Mr. Chairman, for at least some of the discussion that went on during the Q&A.

Mr. SHAYS. Sure.

Mr. FERTEL. I mentioned, and NRC has done their own study, so they can share theirs. But theirs is secret, and ours, we've made public. We've done studies right after September 11th that looked at a 767 hitting the spent fuel pools and a 767 hitting dry cask storage.

And you can go to a bigger airplane, a faster speed, but this was a pretty big plane. It's 80 percent of the air flights we have in this country. And the outcome was there was no release of radiation. There was a very bad day on the plant. There was a lot of damage. There was a lot of——

Mr. SHAYS. The spent fuel that is at Indian Point, is that under the dome?

Mr. FERTEL. Spent fuel at Indian Point is almost impossible to hit, to be honest.

Mr. SHAYS. No, that is not what I asked. Is it under the protected dome?

Mr. FERTEL. It is because it's a pressurized water reactor. It is in a building next to the containment. It's not in containment. It's not in there, no. But it is below ground, the pool itself.

Ms. BRIAN. It has one exposed wall, though. It's not entirely——

Mr. SHAYS. Yes. And I understand. It is on the side of the hill. So it would be harder to hit. But——

Mr. FERTEL. I mean, there's a reality and a theoretical reality to some of these things, and I'm not pooh-poohing where something could happen. What I'm telling you is that has been looked at. NRC has also done these independent studies, which looks at what you can do to protect it, and those studies have been completed. So there has been a lot done looking at spent fuel pools, and appropriately so.

My point is beyond spent fuel pools. It goes to this question of enemy of the state and what's the responsibility of the commercial operator?

Mr. SHAYS. The reason why spent fuel was on the table was that it is our biggest fear is that it becomes a target for an enemy of the state. That is why it was on the table.

Mr. FERTEL. I understand that.

Mr. SHAYS. OK. You wanted to finish your point?

Mr. FERTEL. Yes, my point, sir, is that whether it's an enemy of the state in the conventional definition that the NRC has always had, or maybe in what people believe today, which is just some really bad terrorists that are trying to get us, the response of the private sector ought to be what it's capable of doing, and we shouldn't pretend it can do more. It can't shoot down airplanes.

And what we really need to do is what I think DHS has embarked upon, which is to look at threats that are much bigger than our DBT and to look at threats that are smaller and to risk inform and threat inform how they bring integrated resources to support whatever you have. And that is going on.

Mr. SHAYS. It seems logical what you say what the industry is capable of doing. But there is an assumption that the design basis threat will protect the plant and, therefore, the public. That is the assumption.

So the assumption is that whatever is required, the plant will be protected. What the inference of your comment is that if it is not capable of doing it, then we don't require it to do it. Therefore, it is not part of the design basis threat. That is the inference of your comment.

Mr. FERTEL. Our understanding of the design basis threat—and you have a Commissioner here, so he can give you theirs—is that the design basis threat is what the NRC holds licensees accountable at a high assurance to ensure that they can defend against.

It is not the full spectrum of threats. It is not the most credible threat necessarily. It could be bigger or smaller than the most credible threat. But it is what they believe licensees need to be able to with high assurance win at. And we believe there is threats that go beyond that.

Mr. SHAYS. Right.

Mr. FERTEL. And that those need to be dealt with not necessarily because it's an enemy of the state, but because as a country right now we are standing up a system that's attempting to protect our whole critical infrastructure. Not just nuclear plants, but everything else, and how do we do that?

And to be honest, I think DHS is moving down a responsible road maybe too slowly.

Mr. SHAYS. Well, definitely too slowly.

Mr. FERTEL. Yes, I would agree.

Mr. SHAYS. Maybe Mr. Blumenthal, you could jump in in just 1 second. But what the inference to the public is that a design basis threat meets the threat. Therefore, you are protected. And the inference from your statement is the design basis threat meets the capability of the industry at a particular site to do what it is capable of doing, but it doesn't necessarily meet the threat.

Mr. FERTEL. I'd say it just slightly different. If it's my words, I'd say it's what the NRC has decided that the industry individual licensees must meet with high assurance of winning. They decide it. We don't decide it. They do.

Mr. SHAYS. Yes. How do you react to this dialog, Mr. Blumenthal? Mr. Blumenthal, I would like you to respond to what you are hearing being said.

Mr. BLUMENTHAL. Well, you know, I was just looking through some of my notes about what Chairman Diaz said.

Mr. SHAYS. So you were taking notes? You weren't just sitting there. [Laughter.]

Mr. BLUMENTHAL. Let me react in this way. If someone had predicted on September 10, 2001, that the two buildings of the World Trade Center would not only be hit, but would come down, there would have been a lot of engineers who would have said, "No way. You can hit them 10 different times, 10 different ways, and they will stand, and people will exit them."

If you had said somebody flying an aircraft is going to try to hit a nuclear plant in Pennsylvania or the Pentagon, they would have said, "No way. But even if they do, they won't do damage."

And I guess the question is not whether a terrorist can hit a spent fuel pool. Certainly, we know that is possible. The question is, first, can they be stopped? And second, what damage will be done?

And my own military experience leads me to think that kind of attack should prompt action on all fronts. That is from the plant operator, who should design it not just to withstand what is a couple of studies in terms of prediction of damage, but should be designed to be as damage proof as possible under all circumstances. And I don't think we have any assurance that the plant operators have been required to build as strongly and hardly as possible.

And of course, the military, the Federal Government has an obligation, too. You want a belt and suspenders type of approach here. You don't want to just say, well, that is the Federal Government's responsibility, or the nuclear plant operator ought to build it so that it can withstand attack no matter what. Both ought to be focused on this problem.

I just think that's one reason why this distinction is artificial and outmoded and unrealistic.

Ms. BRIAN. If I could make a point that may clarify my vision of why I think this is ridiculous?

Mr. SHAYS. Sure.

Ms. BRIAN. This attack, if it were to happen, the tests have shown there are sort of 3 to 8 minutes, very fast. Quick. You either win or you lose. And it also takes, studies have shown or tests have shown, about an hour and a half or 2 hours to get a SWAT team, get them together, assembled, put all their equipment on, brief them, get them there.

There's this giant gap, and the gap is essentially created by this distinction of enemy of the state. I'm not suggesting that the people at the plant are going to say, "I'm not going to fight." But the point is the things they're no longer required to protect against is because it's been deemed an enemy of the state type weapon or method.

And that's a distinction that I think we have this cavern of time, which I understand DHS is theoretically shrinking, but that's a huge cavern that I think is the Government's responsibility to do something about if industry isn't being asked to do it.

Mr. FERTEL. Just on Danielle's statement. Part of the comprehensive reviews that DHS is doing is looking at exactly what she's referring to. They are looking at the threat spectrum at every plant, and basically, they have a series of 16 big threats they look at.

Then they're looking to see if they thought that a ground assault, which is what you're referring to, of a large force—which is one of their—in fact, a lot of their threats are very large forces—was likely in that area, they're looking at what they would have to do to help prevent it, to help you identify it sooner because these things don't happen overnight.

The experts are going to be doing surveillance and everything else. They're actually sitting down and thinking through if my site was one where they thought that could happen, what would they be giving local law enforcement to state, and what would they be setting up to protect the site not when it's attacked, but to give them early warning that you're under surveillance and stuff like that? And then to think about attack and take-back.

Another study that we did, and it goes to Danielle's statement, if you lose. This was at a request for us to take a look at a ground assault that actually won and was able to get into the plant, was able to cause a release of radiation. And I wouldn't profess that this is a good outcome, but the outcome is not nearly as dramatic, at least in death, as one normally hypothesizes.

What it found was there would be two prompt fatalities, and we can make this available to the subcommittee, if you'd like, Mr. Chairman. And there would be about 100 latent cancers over the long term, which would not statistically change the cancer rate in an area.

And this was done for a real plant situation with a population that was relatively large around it. It was not a specific plant. We were not asked to try and do it for a specific plant so that people could get scared. It was putting together a couple of situations. We'd be more than glad to share it.

I'm not at all professing that's an acceptable outcome. What I'm trying to point out is that the consequences of some of these things I think are much greater in people's mind than potentially in reality, though we should make sure it never happens.

Mr. SHAYS. When we meet, is it next month? Do you have a hearing schedule? When we have our hearing in May behind closed doors, what would be the questions that you would want to ask, Mr. Blumenthal and Ms. Brian, if you were me in those hearings?

Ms. BRIAN. OK. I would love you to ask the Commissioners if they think that everything is being reasonably asked of industry because I don't believe the Commission——

Mr. SHAYS. Well, I could ask that in open forum. Give me something exciting to ask.

Ms. BRIAN. Well, ask them why they are not protecting against weapons that we know terrorists use all the time.

Mr. BLUMENTHAL. I'd like to know what weapons have been eliminated, what specific weapons have been eliminated and why. What additional weapons, apart from the recommendations as to what should be considered, what additional weapons staff has con-

sidered as relevant to that kind of attack and why they haven't even been considered by the staff?

And what studies have been done by them, not by the industry, but by the Nuclear Regulatory Commission that show we shouldn't be worried about spent fuel pools and why they're sufficiently protected?

Mr. SHAYS. When they had the general concept in the Department of Energy on the design basis threat, when we were there, we had concern that they were focused too much on someone getting in and out.

September 11th answered that question. A lot of people don't care if they go up with whatever. In other words, they don't care if they die in the process of causing a real catastrophe.

So, Mr. Fertel and Mr. Crane, you would agree that the design basis threat, based on that, had to go up significantly. Correct?

Mr. CRANE. Yes, I agree, and it did.

Mr. SHAYS. Now the other issue was whether you had, there is a huge difference between whether you had one insider or two. Obviously, I could carry it to extremes. I mean, I happen to believe when you cut taxes, you generate economic activity. But obviously, if you got rid of all taxes, that is carrying it to the extreme.

So I could carry this to the extreme. But I happen to believe it is very likely you would have more than one insider. Would you agree that with every inside person the task becomes much more difficult, and especially depending on who the insider would be and what capacity?

Mr. CRANE. I think that you can come up with scenarios that could create tougher situations, and that's why we have to depend on more than just the guard force to ensure that the insider threat is minimized—through constant behavioral assessments, through different psychological tools. Members of our staff that have that critical knowledge have an enhanced inspection characteristic and behavioral assessments done on them, and their background evaluations are reviewed more frequently.

So the answer is yes. You could come up with scenarios that could make it very tough. The guard forces, the guard force, they are very well trained. But we have other administrative tools to ensure that does not happen.

Ms. BRIAN. Congressman, if you could also ask them about the number of attackers they are protecting against?

Mr. SHAYS. Well, that was the other issue when we were looking at Y–12.

Ms. BRIAN. Right.

Mr. SHAYS. We felt originally that they were underestimating the number of people potentially who could, and when they increased the numbers, obviously, it became a much more difficult challenge for them.

What I would also want to know is obviously everything that they changed from staff to once they interacted. And we can be very candid publicly our reaction as to whether we felt that this was influenced too much by the concept that I know is legitimate. But that also can be carried to an extreme, and what is the industry capable of doing?

What I am left with in this hearing, and maybe you could react to it? I am left with a feeling that I had come to this hearing thinking that the design basis threat was pretty much, if we met it, we could pretty much protect a facility.

I am leaving with the view that the design basis threat is a logical thing to do to maximize our capability to respond to an attack, but even if we meet it, it is no guarantee that we have protected the plant because it may be in some plants that it is simply not practical to do everything you need to do to fully protect it.

That is where I want to kind of have a dialog behind closed doors as to whether that happens at all or whether it happens, you know, often. Because obviously we can't ask you to do something you can't do.

But it seems to me that the threat has to be realistic, whatever it is. And then the chips fall where they may. And I am wondering, and maybe I could ask you, Commissioner, to just step up for this? If you didn't mind, just pulling a chair up?

And if your colleagues are disappointed they aren't here to give a different view, you could tell them they could have stayed, if that is not too fresh.

Mr. MCGAFFIGAN. I was the designated Commissioner.

Mr. SHAYS. Good. Well, then that is super. Thank you.

Then we will assume that you are speaking for the Commission. Did you hear my last basic point?

Mr. MCGAFFIGAN. Yes.

Mr. SHAYS. Yes, maybe you could respond to it?

Mr. MCGAFFIGAN. Sir, I think it's permeated the hearing today. Clearly, there are threats that go beyond the design basis threat. I talked earlier about the aircraft threat and what we have done with NORAD.

Mr. SHAYS. Yes, but let us get rid of the airplane.

Mr. MCGAFFIGAN. But I also think that the comprehensive reviews, although they're paper exercises to some degree, show that the capability of our guard forces, which is really extraordinary. I'd encourage you to visit Millstone or Indian Point. Or as I said, I was at Quad Cities last week. They are pretty extraordinary forces.

I'll give you unclassified numbers. There are 8,000 guards at approximately 64 sites. That means 125 per site. That means about 25 per shift on average. There are some sites that have more, some that have less. So you're attacking a site that has 25 people armed with AR–15s and other sort of weapons, lots of ammunition in prepared positions that you have taken on.

I would argue that our regulatory requirement is high assurance that during an exercise they can defend against the DBT. I think they have extraordinary capability against beyond DBT ground-type assaults and that the capability degrades gracefully, and it isn't a matter that if you have—and we've tested it at one site.

I mean we'd like to have more industry volunteers, and I'll put in that plug right now. But one site we tested 2X, and the site did just fine. Against twice the size of the force. That particular site had no targets that's destroyed. They destroyed twice as many guards.

We think that would happen more frequently. It is hard, the industry always is wary of the regulator in terms of allowing us to

explore beyond regulatory threats. But I say I think it degrades gracefully.

And then for the extraordinary threats like the aircraft, we do two things. We work with NORAD, and we invoke our safety authorities, whether it's a spent fuel pool or a core. We assume the worst, and say, OK, what can you guys do now to mitigate it, to prevent anybody offsite from being hurt?

Mr. SHAYS. What I think what we may end up having to do that might make industry very uncomfortable. I am going to say to you that I happen to think ultimately the environmental movement, to which I feel very close to, is ultimately going to have to decide whether we want global warming or nuclear generating power plants in addition to conservation.

I think that it is going to be whether we are going to be competitive with the rest of the world as they end up with nuclear plants on a generating plants. I mean, I happen to believe that we are going to have plants in this country, and I vote to send it to Yucca Mountain.

But I am uncomfortable with having plants until we decide what we do with spent fuel. I don't like the idea, I think we are very vulnerable leaving them onsite. So I have some discomforts.

But it seems to me that we almost need to have another way to grade every plan and say this is the extent to which the design basis threat is feasible and logical. I believe that we have made a decision to lower the design basis threat because it is not practical to meet what may, in fact, be a very realistic threat.

I believe that is true. Obviously, that is debatable. But I think that there are scenarios that would almost be impractical for a plant to have prepared for 24 hours a day. But I believe also that the design basis threat gives people a sense that if, in fact, we need it, whatever that is, that people feel we are protected. And I don't think we are because I think we do compromise it.

So then the issue to me is, should there be another way to which we then inform at least, if not publicly, those decisionmakers that this plant isn't as well protected and can never be as well protected as this plant because it is impractical to do all the things that we have to do at this plant?

And then have a private dialog in particular about what that means. Is this something that ever happens in dialog——

Mr. MCGAFFIGAN. Mr. Chairman, in terms of looking at new plants, the Commission last summer, when I was off the Commission briefly waiting to be reconfirmed, did make a decision that we would ask for a so-called target set analysis of each of the new designs as part of our process.

We believe that the target set is the set of equipment that you have to take out in order to lead to core damage or to—we were focused on the core or to spent fuel damage. The more complicated, the larger the target set, the more the terrorist has to do to succeed, the less the probability of the terrorist succeeding.

And a lot of that can be built into the design, and I believe it's already built into the design of each of the new reactors—the AP1000, the Economic Simplified Boiling Water Reactor, and the EPR, the European Pressurized Reactor, or whatever they're calling it in the United States these days. They have a different title.

The evolutionary power reactor. Part of their marketing in the United States is to delete "European" and put in "evolutionary."

But each of those, each of those reactors is from a point of view of terrorist attack, we believe, going to be much safer and more secure than the current generation of reactors. Not that the current generation isn't secure, but one of the policy statements the Commission issued a long time ago is that when we embark on a new generation of reactors, they will be both safer and more secure than the current generation of reactors.

We think that will be the case. So, we'll have to be behind the doors that the details of those analyses they're going to give us, but we'll be happy to share those with the Congress, you know, and convince you that these are very secure facilities that are being proposed by the industry.

Mr. SHAYS. And I am exposing my ignorance here, which I do quite often, but I do learn from it. Do we grade every nuclear power-generating plant on a scale of whatever to be able to compare its vulnerability versus another one?

Mr. MCGAFFIGAN. We do not, sir.

Mr. SHAYS. That to me seems—what?

Mr. MCGAFFIGAN. We have studies and these comprehensive reviews——

Mr. SHAYS. But I think you know where I am going. Before you answer, I would just tell you where I am going. Where I am going is, obviously, that would have to be kept very confidential because you then don't want to expose it to the adversaries.

But if the logic is that someone goes to the weakest target, what is the weakest one? And some have to be weaker than others. And if they are not weaker, maybe their consequence is greater if—just hold on 1 second. You will get your chance.

The consequence may be even worse. I mean, maybe one plant isn't as vulnerable, but if it is hit in an effective way, the consequence is far greater than the weaker plant, if you get my gist here?

But it would seem to me that we would grade every plant, we would know how each one. And if, in fact, the design basis threat doesn't really meet the actual threat, but what we are capable of meeting, if that is my suspicion and it is right, then it would seem to me we would have to have some way to say this is the vulnerability at this plant?

Mr. FERTEL. Yes, Mr. Chairman. Commissioner McGaffigan referred to it, and I did in my testimony. DHS is on that path. That's exactly what this RAMCAP program does, but not just for nuclear plants, it does it for LNG facilities. It's going to do it for chemical plants. It's going to do it for all the critical infrastructure sectors.

And what they do is they go out and they have a spectrum of 16 threats, and you should have them come in and tell you what they're doing.

Now they don't necessarily say this is a credible threat and this is a noncredible threat. They look at all of them, and they ask for the worst-case consequences for each of those. Not a very sophisticated engineering analysis, more qualitative. But they have a methodology they use that gives them pretty good data and prob-

ably for nuclear plants gives them the best data because there's been so much done at those plants.

Their intent, and they've got to get to execution, they're doing the things now. Their intent was that they would then have a matrix for all of the critical infrastructure. So my nuclear plant, Danielle's chemical plant, attorney general's LNG facility. And they would look at these 16 threats.

Mr. SHAYS. I don't think you would want to be associated with an LNG. [Laughter.]

Mr. BLUMENTHAL. I'm taking it in the spirit that it was offered.

Mr. FERTEL. It was inclusiveness.

Mr. BLUMENTHAL. He's not giving me ownership.

Mr. FERTEL. What they would be doing is they would be saying that for threat A, we think there's a high likelihood that may occur in our country. And they would look and they'd say, OK, threat A has very low consequence for my facility, but high consequence for Danielle's.

They would then look and say do we feel we're adequately protected as a Nation? Not as her as a separate entity, but with what she's doing at her plant and what the Federal Government and State and local are going to do, what else do they need to do to enhance the margin of security?

That's the effort that they're on, and it's a combination of this RAMCAP, plus what Commissioner McGaffigan referred to on comprehensive reviews. That is the closest thing to what you're discussing, but it's not ranking nuclear plants among nuclear plants. It's ranking nuclear plants within the infrastructure. And some nuclear will be high risk you need to deal with, and some will be very low risk.

Mr. BLUMENTHAL. If I can just interject, as a non-expert, as just a——

Mr. SHAYS. Why don't you just say as an unbiased person?

Mr. BLUMENTHAL. As a country lawyer.

Mr. SHAYS. OK. Yes, right. [Laughter.]

Mr. BLUMENTHAL. You know, as I listen to all of the terminology and the reports about studies and the consideration of threat levels and all the rest of it, I'm struck by the need to have perhaps some agency other than the NRC doing these security assessments. And maybe it should be the homeland security agency.

But one of my main reasons for being tempted by that outcome is the account from the GAO, which I think is absolutely stunning that the design basis threat was redefined because the industry objected to the expense of it being responsible for protecting against certain weapons. It, in effect, persuaded the NRC to redefine this design basis threat because of its needs, financially and otherwise.

And you know, the security of our nuclear plants maybe is too important for the Nuclear Regulatory Commission to be responsible for performing or assuring.

Mr. SHAYS. I would tend to agree, especially if we start to see more of them, more plants.

Mr. BLUMENTHAL. And I want to——

Mr. SHAYS. You will get that in——

Mr. BLUMENTHAL. I realize that it may seem like a novel or dramatic idea, but——

Mr. SHAYS. I don't think it is novel, actually.

Mr. BLUMENTHAL. Not novel?

Mr. SHAYS. No. Not novel.

Mr. BLUMENTHAL. Well, that gives me some assurance. [Laughter.]

And I didn't suggest that it was entirely novel, but novel for the——

Mr. SHAYS. In this room, it seems novel right now, yes.

Mr. BLUMENTHAL [continuing]. Congress to consider doing. But certainly where the lack of transparency, which, again, the GAO highlighted. Where you have lack of transparency and apparent possible over-involvement of the industry, you would want a different agency to be making these decisions.

Mr. SHAYS. Right. I hear you.

Yes, Commissioner?

So now we are going to close up.

Mr. MCGAFFIGAN. Two points. One is in response to your original question, the ranking. Rankings, just if we did safety rankings of the 103 plants, it would depend on the configuration of the plant at any given point in time, and it's the same in security.

So one plant may be more secure than another at time X and not be more secure at time Y, depending on what else is happening at the plant at the same time. So it's a complicated thing.

To the extent that we can, we do provide NORAD and NORTHCOM—and we can talk to you about this in a classified meeting—our list of things they should focus on, and we give them plant status on critical parameters so that they can better assign their resources. We do that. We've done that already. We've been doing that for years.

On the issue of independence of the Nuclear Regulatory Commission, all I can say, sir, is that our staff is a very professional group of folks. They are not lapdogs of the industry or wholly owned subsidiaries of NEI.

I have personally had no ties to this industry throughout my life. I'm a 30-year civil servant. I worked for Jeff Bingaman for 14 years. I was a Foreign Service officer for 7 years. I have never collected a check except from Harvard, CalTech, and the Federal Government, U.S. Treasury. And most of our staff is exactly that way.

Some Commissioners have ties to the industry. I think that's a different—they bring a perspective. And you benefit—we are an independent regulator. We are the watchdog.

I wish, one thing, sir, if you're ever working on the title of the Nuclear Regulatory Commission, I wish we were called the Nuclear Safety and Security Commission because "regulatory" has such a negative connotation in our society, and most other——

Mr. SHAYS. Well, names do matter. We do have the Patriot Act.

Mr. MCGAFFIGAN. Yes, I know. Names do matter. And most other regulatory bodies on the face of the Earth have "safety" in their title, and we, unfortunately, have "regulatory," which brings with it all those negative connotations.

We are an independent body. We call the shots, the balls and strikes, as we see them. These folks are put through their paces that are our licensees in both safety and security.

Mr. SHAYS. I hear you. Now I understand why they allowed you to stay. [Laughter.]

Mr. Crane.

Mr. CRANE. I just have to——

Mr. SHAYS. I don't mean allowed, asked you to stay.

Mr. CRANE. I just have to respond to a couple of comments.

Mr. SHAYS. Sure.

Mr. CRANE. First of all, I think most regulatory agencies have stakeholder interface meetings and conversations, and I think it's a critical part to make sure you hit the mark when the regulation comes up.

The NRC did afford a small section of the industry that was a working group to be able to look at the feasibility of what could be done not only in the timeline of what could be done or what reasonably we had to protect ourselves again. Probabilities came into our feedback.

We are not an industry that is overly driven by profits, and we have not been pushing back overly hard. We have spent over $1.2 billion. There are 16 sectors in the United States, and show one other sector that's put anywhere near that money into it and voluntarily done this and expedited it.

At our company alone, we've spent over $140 million in a very short period, a 1-year period of time, $140 million, and we increased our operational expenses by 100 percent. We didn't go ask for handouts from Congress. We didn't ask for handouts from Homeland Security.

We are dedicated to protecting our people. We are dedicated to protecting our assets. If we cut a corner in our industry, billions of dollars of value of our shareholders are lost immediately. So to portray us as being able to push back on the regulator and we're driven by money is totally false.

Mr. SHAYS. No. And that extreme statement would be false. But having been in this business of Government for 30 years, you do have competing interests.

And I think that the issue is to what extent do you want to protect yourself? And I think that is where you would have an industry that might think 10 years, but maybe not think of the 30-year case, or the 30-year storm or whatever. So I think it is somewhere in between.

I think people have been, frankly, pretty respectful of your industry and here as well. And let me just say I would like to end this hearing, if I could, by allowing each of you to make any point that you think, question that we should have asked that we didn't or any point that you want to put on the record before we adjourn.

And maybe I will start with you, Mr. Blumenthal, and give Mr. Crane a chance to think about it.

Mr. BLUMENTHAL. Well, my point is going to be very brief because I have to catch a plane to be back in Connecticut for a commitment. So I'm willing to defer. I yield my time, as the saying goes in Congress.

Mr. SHAYS. OK. Ms. Brian.

Thank you, sir.

Ms. BRIAN. I would just want to add that——

Mr. BLUMENTHAL. Excuse me for interrupting. I really do want to thank you, Mr. Chairman, for having this hearing, which I think has really been very useful and important.

Mr. SHAYS. Thank you.

Mr. BLUMENTHAL. As well as your subcommittee and for all the great work you're doing.

Mr. SHAYS. Thank you very much. You know what? Why don't you just feel free to leave right now? Honestly, because I am just going to go down. So, thank you so much.

Mr. BLUMENTHAL. Thank you.

Mr. SHAYS. Travel safe.

Yes, ma'am?

Ms. BRIAN. I only wanted to add the reminder that in the process that this took place, where the staff was able to work with industry and come up with some changes in their recommendations, other people aren't allowed in that process because only very few people have the clearance and the capacity.

So those of us on the outside are allowed to submit comments, but we're blindfolded because we're commenting on things that we're not allowed to know about.

Mr. SHAYS. Thank you.

Mr. Fertel.

Mr. FERTEL. I think the thing I would encourage, Mr. Chairman, is for you to be briefed by DHS on what they're doing more broadly to protect the critical infrastructure. I think it goes to the heart of the some of the issues and concerns you've raised.

Mr. SHAYS. Well, I hope this won't shock you, but I have more faith in the NRC than I do in DHS. So——

Mr. FERTEL. It doesn't shock me, and again, I'm not trying to defend them. But I'm just saying they are doing something.

Mr. SHAYS. In fact, let me say this to you—a lot more confidence. So that tells you where I am at.

Mr. FERTEL. But you helped create them, so we should try to make them effective.

Mr. SHAYS. No, and there will be a point in time where they will get better and better and better. But you know, I am still trying to sort out Katrina. We didn't want them to stand by, watching FEMA fail. We wanted them to be proactive and help FEMA.

Mr. CRANE. That was going to be my same comment on anything you could do for us with DHS to expedite, it would be helpful.

Mr. SHAYS. OK. Great. I think you all have been wonderful witnesses.

And I am going to note for the record the NRC has evidently made a greater effort to be cooperative with our people that look at them, which is I think Ms. Brian's request, and I think that is a positive thing.

But, Ms. Brian, we need organizations like yours to be speaking out and raising concerns, and we thank you for that. And we appreciate the work of the industry. So thank you all very much.

Ms. BRIAN. Thank you, Chairman.

Mr. SHAYS. Thank you, Commissioner.

This hearing is adjourned.

[Whereupon, at 5:15 p.m., the subcommittee was adjourned.]

○